8
24-76
25 Sept 77
Specs Distrib

~~24-76~~
no stock

BNWL-1959
UC-70

MASTER

A Risk-based Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accidental Release Sequences in Nuclear Fuel Cycle Operations

January 1976

Prepared for the U.S. Energy
Research and Development Administration
under Contract AT(45-1):1830

Battelle

Pacific Northwest Laboratories

BNWL-1959

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

PACIFIC NORTHWEST LABORATORY
operated by
BATTELLE
for the
U.S. ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION
Under Contract E(45-1)-1830

Printed in the United States of America
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22151
Price: Printed Copy \$4.00; Microfiche \$2.25

ERRATA

- Page iv The title of 7.4.3.2 should read: "...on Event Chain Length"
- Page 47 Add to line 4: The relatively large value of n_{cut} stems from liberal use of inhibit gates with probabilities on the order of 10^{-1} . The unique terms are therefore not all independent basic events.
- Page 47 Line 21 should read: "...the curve of minimal cut sets..."
- Page 56 In line 18 delete the lower comma after CP_{j_2} .
- Page 72 Line 12 should read: "...an upper bound..."
- Page 84 Line 2 should read: "...a differential form..."
- Page D.2 In Equation 5, the quantity " $\geq A(n)$ " should be elevated to the level of the body of the equation.
- Page E.4 In line 15 the quantity should read: " $E(c_i | S_i)$."

A RISK-BASED FAULT TREE ANALYSIS METHOD
FOR IDENTIFICATION, PRELIMINARY EVALUATION,
AND SCREENING OF POTENTIAL ACCIDENTAL RELEASE
SEQUENCES IN NUCLEAR FUEL CYCLE OPERATIONS

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

by
T. H. Smith
P. J. Peltó
D. L. Stevens
G. D. Seybold
W. L. Purcell
L. V. Kimmel

January 1976

Battelle
Pacific Northwest Laboratories
Richland, Washington 99352

ACKNOWLEDGMENTS

Significant contributions by the following people to the preparation and review of this report are gratefully acknowledged: Dr. S. C. Saunders developed the treatment of unidentified failure sequences presented in Appendix K. Dr. J. L. Carter, Jr., contributed the description in Appendix B of the ACORN computer code which he developed. Many improvements in the report resulted from review by D. F. Haasl, R. K. Weatherwax, Jr., P. A. Crosetti, and Dr. Saunders. Numerous fruitful discussions were held with Mr. Crosetti and with W. J. Van Slyke in the early stages of the study.

CONTENTS

ACKNOWLEDGMENTS	ii
LIST OF FIGURES	vii
LIST OF TABLES	viii
1.0 SUMMARY	1
2.0 INTRODUCTION	5
3.0 PRELIMINARY ANALYSES	9
4.0 SYSTEMATIC IDENTIFICATION OF POTENTIAL RELEASE SEQUENCES	11
4.1 Introduction	11
4.2 The Web of Events	11
4.3 How Various Systems Safety Methods Handle the Web of Events	13
4.4 Selection of a Systems Safety Method	15
4.5 Summary of the Technique Selected for Constructing Fault Trees	17
4.6 Treatment of Nonbinary Events	19
4.7 Critical Review of Fault Trees After Their Construction	21
5.0 SIMPLIFICATION OF THE ANALYSIS OF LARGE FAULT TREES	23
5.1 The Task of Analyzing Large Fault Trees	23
5.2 Possible Solutions to the Problem	23
5.3 Development and Demonstration of a Screening Method	24
6.0 STATEMENT AND SIMPLIFICATION OF THE RISK EQUATION	27
6.1 Basic Considerations in Screening	27
6.2 Stating the Risk Equation	28
6.3 Simplification of the Risk Equation	29
6.3.1 Objective	29
6.3.2 Elimination of E	30
6.3.3 Grouping on the Basis of D	30
6.3.4 Treatment of the C Term	32
6.3.5 Result	35

CONTENTS (contd)

7.0	PROCEDURE FOR SCREENING CUT SETS, BASED ON A x B VALUES	37
7.1	Selection of Screening Technique	37
7.1.1	Manual Evaluation	37
7.1.2	Monte Carlo Fault Tree Codes	37
7.1.3	Analytical Fault Tree Codes	38
7.2	Summary of the Screening Procedure	38
7.3	Preliminary Simplification of Fault Trees	39
7.4	Derivation of the Cutoff Values	42
7.4.1	Selection of a Reference Cut Set	42
7.4.2	Probability Cutoff	44
7.4.3	Event Chain Length Cutoff	45
7.4.3.1	General Approach	45
7.4.3.2	Calculation of the Cutoff an Event Chain Length	46
7.4.3.3	Savings Achievable by Use of an Event Chain Length Cutoff	47
7.5	Handling the A Term: Cut Set Identification, Probability Calculation, and Screening	50
7.5.1	Code FAULT	50
7.5.1.1	General Function	50
7.5.1.2	Code Capacity	52
7.5.1.3	Probability Calculations	52
7.5.1.4	Cut Set Accounting Procedures	52
7.5.2	Code FAULTG	53
7.5.3	Probability Data	54
7.6	Handling the B Term and the A x B Product	55
7.6.1	Introduction and Summary	55
7.6.2	Calculation of A x B Products by Code RAFT	55
7.6.2.1	Release Fractions	55
7.6.2.2	Total Available Inventory	56
7.6.2.3	Calculational Procedure	57
7.6.3	Difficulties in Assigning Release Fractions	58
7.6.4	Release Fraction Data	60

CONTENTS (contd)

7.7	Checkout of the Computer Codes	60
8.0	THE TOTAL RISK OF THE POTENTIAL RELEASE SEQUENCES OF AN OPERATION	63
8.1	Introduction	63
8.2	The Risk Sum of the Discarded Sequences	64
8.3	The Risk Sum of the Omitted Sequences	67
8.3.1	Definition of the Completeness Problem	67
8.3.2	An Upper Bound on the Actual Risk of a System	70
8.3.3	Verification of Predicted Risk	72
8.3.4	Two Limiting Cases Related to Unidentified Risk.	73
8.3.4.1	The Case of Generic Sequences	73
8.3.4.2	The Case of Additional Risk	75
9.0	AN ALTERNATIVE SCREENING PROCEDURE BASED DIRECTLY ON RISK MEASURE.	79
9.1	Derivation of the Alternative Screening Procedure.	79
9.2	Advantages and Limitations of the Alternative Procedure.	80
10.0	PRELIMINARY EVALUATION AND SCREENING WITH NO ASSUMED FORM OF THE RISK EXPRESSION	83
10.1	Background Regarding Probability, Consequences, Risk, and Value	83
10.2	Modifications Required for the Optional Procedures	85
10.2.1	Determining the Values of A_{cut} and n_{cut}	85
10.2.2	Presenting the Screening Results	87
11.0	DETAILED ANALYSIS PHASE	89
11.1	Overview	89
11.2	Spectrum Considerations	91
11.3	Dependent Events/Common Cause Failures	92
11.3.1	Background	92
11.3.2	Review of Existing Common Cause Failure Methods.	94
11.3.3	A Recommended Approach for Common Cause Failure Analysis	94
11.3.3.1	Points in the Risk Analysis at Which CCF Errors Could Arise.	95
11.3.3.2	Overview of a Proposed Defense Against the Principal CCF Hazards	95

CONTENTS (contd)

11.3.3.3	Outline of a Proposed Procedure for Defending Against the Third CCF Pitfall	96
11.4	Sensitivity and Importance Studies.	99
12.0	REFERENCES	101
APPENDIX A:	Simplified Illustration of the To/Through Technique for Fault Tree Construction	A.1
APPENDIX B:	The ACORN Code for Plotting Fault Trees	B.1
APPENDIX C:	Equations for Evaluating Cut Set and Top Event Probabilities	C.1
APPENDIX D:	Determining the Event Chain Length Cutoff, n_{cut}	D.1
APPENDIX E:	Treatment of Absorption	E.1
APPENDIX F:	Input/Output Description for Fault Tree Analysis Codes FAULT and FAULTG	F.1
APPENDIX G:	Input/Output Description of Code RAFT for Calculation of Release Quantity and Risk Measure	G.1
APPENDIX H:	Specially Constructed Fault Tree for Testing Codes FAULT, FAULTG, and RAFT	H.1
APPENDIX I:	Mathematical Treatment of Dependent Events in Fault Tree Analysis	I.1
APPENDIX J:	Previous Approaches to the Completeness Problem	J.1
APPENDIX K:	Techniques for Estimating the Additional Risk Represented by Unidentified Sequences	K.1
APPENDIX L:	A Fault Tree Illustrating the To/Through Construction Technique	L.1

LIST OF FIGURES

1	Risk Analysis Calculation Flow	6
2	A Simplified Diagram of the Generalized Web of Events for Analysis of Accidental Releases from Facilities	12
3	Use of Preliminary Analysis, Screening, and Detailed Analysis to Obtain Total Calculated Risk for a System	25
4	Illustration of the Effect of C-Term Uncertainties on Comparisons Based on Risk Measure $A \times B$ Only	34
5	Schematic of Screening Process for a Major Branch	40
6	Effect of Screening Process on Risk Analysis Computational Flow	41
7	Distribution of Cut Set Lengths in Several Preliminary Fault Trees	48
8	Accumulation Curves of Cut Set Lengths for Several Preliminary Fault Trees	49
9	Interrelationship of Groups of Potential Failure Sequences	63
10	Calculated Risk as a Function of Time, with Most of the Risk Identified	69
11	Calculated Risk as a Function of Time, with Much of the Risk not Identified	69
12	Upper Confidence Limit on Unreliability	71
13	The Limiting Case in Which All Unidentified Sequences Are Contained Within the More Generic Sequences Which Have Been Identified	74
14	The Limiting Case in Which None of the Unidentified Sequences is a Subdivision of the Identified Sequences	76
15	The Analysis Results Could be Presented as a Histogram of Radionuclide Releases	88
16	Recasting Fault Trees into a Common Form	93
A.1	Barrier Configuration for Simplified Example of the To/Through Technique for Fault Tree Construction	A.1
A.2	Fault Tree Representing Release from the Barrier System of the Preceding Figure.	A.2
L.1	The WFP Preliminary Fault Tree for Solidification of High-level Liquid Waste	L.1

LIST OF TABLES

1	Potential Sources of Common (or Shared) Cause Failure	97
2	Properties Indicating Potential Common Cause Susceptibility	98
3	Common Cause Failure Preventive Measures	98
4	Jacobs' Procedure for CCF Analysis	99
D.1	Basic Events of Highest Probability and Unavailability in the Preliminary Water Basin Storage Fault Tree	D.4
E.1	Potential Release Sequences Demonstrating Possible Absorption Errors in Fault Tree Analysis Used Directly for Risk Studies	E.7
G.1	Input Instructions	G.4

A RISK-BASED FAULT TREE ANALYSIS METHOD FOR IDENTIFICATION,
PRELIMINARY EVALUATION, AND SCREENING OF POTENTIAL ACCIDENTAL RELEASE
SEQUENCES IN NUCLEAR FUEL CYCLE OPERATIONS

T. H. Smith, P. J. Pelto, D. L. Stevens, G. D. Seybold,
W. L. Purcell and L. V. Kimmel

1.0 SUMMARY

A method is described for identification, preliminary evaluation, and screening of potential accident sequences leading to uncontrolled release of radioactive materials. Included is a procedure for estimating the risk sum of all identified sequences.

In addition, portions of the procedures have been developed for detailed analysis of the dominant (highest risk) sequences so screened. Existing methods, such as event trees or cause/consequence diagrams, could also be used for the detailed analysis.

This method was developed for the Energy Research and Development Administration (ERDA)-sponsored risk analysis of systems for managing high-level waste, part of the Waste Fixation Program (WFP). However, the method appears useful for analysis of most operations of the nuclear fuel cycle.

The method begins with certain preliminary analyses. The facility and operation are described and analysis bounds are established. Safety Analysis Reports (SAR) and related documents are reviewed, and a preliminary hazards analysis is performed.

After reviewing several methods for systematic identification of accidental release sequences, a type of fault tree construction, the "to/through" approach, was chosen for the WFP waste management system. Variations of the approach, which resembles the "leak path" approach, have been applied by other investigators to several fuel cycle operations. The top, undesired event (accidental release of radioactive material from the

facility) is postulated. The analyst traces back in reverse sequence to determine how each containment barrier could have been breached. The material must move to each barrier and pass through it for release to occur. The process is continued until initiating events have been reached and all conceivable release sequences of importance postulated.

Although, in theory, different safety analysis methods can give identical results, the to/through fault tree approach offers advantages over others in several respects. It focuses on an undesired event which is closer to the event of ultimate interest. The analysis is considered more complete because the system is treated as a whole. A more direct treatment of common cause failures also results because all events appear on one fault tree. Probability and consequence analyses are more closely coupled. The analysis is more easily displayed on one large diagram.

No assumption of critical initial or intermediate events is required, as in use of event trees and of cause/consequence diagrams, respectively. The critical initiating events for reactors are rather well defined as a result of years of safety analysis. However, for reprocessing plants and other fuel cycle operations, the key initiators are not well known. Numerous potential radioactive sources may exist in various forms and within various containment systems in one facility.

The price paid for these advantages is the required analysis of a very large fault tree. However, this problem has been made tractable by methods described herein.

It is neither feasible nor desirable to evaluate carefully all of the millions of postulated release sequences in large fault trees for complex nuclear systems. The approach adopted was to identify and separate the sequences contributing most to system risk and to concentrate the evaluation on those sequences. The screening decision is based on a measure of risk, not simply on probability. An approximate risk sum of the discarded sequences is retained for later addition, giving the total estimated risk for the system as characterized by the fault tree.

By separating the dominant from the low-risk sequences, the screening identifies, early in the study, major potential weaknesses in the system,

controlling parameters, and R&D needs. This information is of particular interest for systems in the conceptual design stage.

The screening is based on simplification of a complete risk expression. The risk of a radionuclide release can be thought of as a mathematical product of five terms in appropriate units: A) the probability of the release sequence; B) the release magnitude; C) measures of the physical, chemical, and radiological characteristics of the released material; D) a measure of the environmental transport path efficiency; and E) a measure of the population distribution, characteristics, and habits. An F term for conversion from dose to health effects is optional, as is a G term for conversion to monetary units of loss.

For only comparing and screening sequences within a fault tree for one facility at one site, the risk expression can be simplified. The E term (population density) is generally independent of failure sequence. Sequences with similar D (environmental transport) terms are grouped and compared only within a group. The C term (material characteristics) can be handled by grouping sequences with similar C terms, or by including C terms with the B terms for release magnitude, or, in some cases, by neglecting small differences and using a sliding (rather than sharp) cutoff to account for uncertainties.

Under these conditions, screening and preliminary ranking of sequences can be conducted within similar groups, based simply on approximate $A \times B$ comparisons. After sequences are identified, probabilities (A terms) are calculated using available data and extensions of WASH-1400 equations. The number of sequences evaluated is reduced by means of derived, not arbitrary, cutoffs on the number of unique events in a sequence and on sequence probability. These calculations are performed by the PNL-developed code FAULTG. The results are fed into the PNL-developed code RAFT, which calculates release quantities (B terms) and ranks sequences on these preliminary $A \times B$ values.

The screening process was successfully demonstrated on a conceptual waste management system for the Waste Fixation Program. Fault trees were

constructed and evaluated for processing, handling, transporting, and storing high-level waste. Trees of up to 14,000,000 release sequences (BICS-Boolean-indicated cut sets) were screened and the top few hundred or thousand sequences preliminarily ranked. Computer time requirements were 1 to 5 minutes on the Cyber 74 per million BICS. An estimate of the total risk represented in the fault tree was also obtained.

We emphasize that the aim of this method, described in Sections 3 through 8, is to determine, by means of comprehensive but approximate calculations, which sequences are potentially the greatest risk contributors and merit further study. Good assurance is thereby provided that one has systematically covered the entire facility or operation before commencing in-depth study of specific sequences. The method is, therefore, particularly useful for complex facilities wherein the dominant sequences or initiating events, in terms of probability and consequences, are not readily apparent beforehand.

The preliminary evaluation and screening can also be accomplished without assuming a specific risk expression (e.g., the product of probability and consequences). The analysis results can be presented in the histogram format of WASH-1400. These optional procedures are described in Section 10.

The preliminary risk measures ($A \times B$) as calculated are not intended to constitute a final effort at risk assessment. Detailed probability and consequence studies of dominant sequences should follow. These studies can involve hand calculations, further use of fault trees, or use of event trees or cause/consequence diagrams. PNL methods developed to date for detailed analysis of the identified dominant sequences are discussed in Section 11.

2.0 INTRODUCTION

Battelle, PNL is performing safety evaluations of high-level waste management systems for the ERDA Waste Fixation Program (WFP). The study is in the form of a quantitative risk analysis of a representative series of processing, storage, handling, and transportation operations.

For each operation, potential accidental release sequences (combinations of events leading to uncontrolled release of radioactive material to the environment) are being analyzed by relating release probability to release consequences. The risk relationship used is the product of the probability of accidental release and the radiological consequences (in dose units) of release. Risk, therefore, is expressed as the mathematically expected radiation dose in a given time period. (Other measures of risk have been proposed. Section 10 discusses changes required in the present method to accommodate a modified risk function or even the absence of a risk function.)

The calculational flow selected for risk analysis is shown schematically in Figure 1.⁽¹⁾ To estimate release consequences, several items must be defined or determined:

- the radioactive source
- its means of confinement
- potential release sequences
- the quantity and characteristics of material released by each postulated incident
- the environmental transport mechanisms
- the exposure pathways.

Estimates of release probabilities constitute the other major effort. An overview of the selected approach has been presented,⁽¹⁾ along with a discussion of problem areas.

The method used for the environmental transport and the exposure phases of the consequences analysis⁽²⁾ closely parallels those of similar studies. However, the airborne particulate modeling includes particle deposition and resuspension. Groundwater transport modeling⁽³⁾ includes radionuclide sorption, diffusion, convection, and generation and decay in soil columns.

FIGURE 1. Risk Analysis Calculation Flow⁽¹⁾

This report discusses the method developed for analyzing potential release sequences. Four analytical phases are involved: 1) preliminary defining and bounding efforts; 2) systematic identification of release sequences; 3) screening of the myriad of sequences to establish the major contributors to the risk (not the release probability) of the system; and 4) refined analysis of the probability and consequences of sequences which survive the screening process.

Methods are not completely developed for the fourth phase of analysis. Section 11 discusses those developed to date. Portions of the anticipated mathematical treatment for the refined analysis have been published,⁽⁴⁾ along with part of the literature review of risk analysis methods.

The remainder of this report discusses the method developed for the first three phases. Included are descriptions of the advanced computer codes for implementation of the method.

It is felt that the present study has made unique contributions in some areas of nuclear safety methods. In other areas, ideas developed by previous investigators have been incorporated. To avoid repetition in this report, those aspects of the analysis which follow previously published methods are not detailed here.

The reader is directed to References 5 and 6 and other sources for background material concerning systems safety analysis. In certain respects, the present fault tree techniques follow those of Reference 7, Appendix II (Volume 1), recommended as background material. Topics of particular interest include: system failure definition; fault tree construction; common mode failures; general approach to quantitative fault tree analysis; Boolean algebra and probability theory; utilization of data; component and primary event quantification; unavailability contributions; and cumulative failure probability.

Risk analysis of nuclear operations is not yet mature. Certainly one cannot identify one method, among the many in use, as being universally superior. On the contrary, our studies indicate that different approaches

may be most appropriate for analyzing different nuclear operations or for different analytical phases of a study. Also, the selection of method should consider the purpose and depth of the study and the backgrounds of the analysts.

3.0 PRELIMINARY ANALYSES

Before systematic identification of potential release sequences, several preliminary analyses are performed. These analyses constitute an important phase of the method. In many respects, the accuracy with which the remainder of the study can be performed is limited by the rigor of the preliminary analyses.

The facility and its operation are delineated, in writing and in drawings, in sufficient detail for the purposes of the analysis. Especially carefully described are the radionuclide inventories (potential source terms) and the barriers designed to contain or control them.

To expedite the analysis, system bounds are established in space (geographic boundaries of the system studied), time (time period studied), and limit of resolution (depth of the study as to system detail).⁽⁵⁾ Component interactions below the limit of resolution will be missed. It is also possible to overlook events which cross the system boundaries. An example is a containment degradation which occurs in a previous operation, but whose effects do not appear prior to the operation under study.

The scope of the study may also be restricted. For example, at present, events such as facility sabotage and material diversion are identified to signal their possible importance. But they are not pursued because of lack of definitive data or of assignment to perform such studies.

Safety Analysis Reports and related documents are reviewed to alert the analyst to system hazards already identified. This review later serves as a check on the completeness of the process of release sequence identification.

The next step is to list hazardous elements in the system, the qualitative significance of potential accidents, and measures provided or recommended for prevention and control. This may be done through a preliminary hazard analysis and expanded upon by means of a fault hazard analysis or a failure modes and effects analysis.^(6,8) Each of these techniques is a single-thread (considers each outcome independent of the others) inductive

type of analysis. In the present method, a preliminary hazard analysis of the system is performed. Again this alerts the analyst to system hazards and later checks the completeness of the systematic search for potential release sequences, the next analytical phase.

4.0 SYSTEMATIC IDENTIFICATION OF POTENTIAL RELEASE SEQUENCES

4.1 INTRODUCTION

Information from hazard analyses is useful in the next analytical phase, use of more powerful inductive or deductive methods to systematically identify potential release sequences. The sequences are also at least preliminarily quantified, in terms of effects and of probability of occurrence. The methods examined include: event trees alone; event trees, with fault trees used to supply most of the branch probabilities;⁽⁷⁾ the similar cause/consequence analysis⁽⁹⁻¹²⁾ in which a fault tree feeds into an event tree through a common critical event and in which fault trees again supply most of the branch probabilities; and various fault tree techniques.

Inductive methods, such as event trees,^(6,7,9-12) start with an assumed initial failure. Additional component failures required to obtain a release (system failure) are then identified. Fault tree analysis,⁽⁵⁻¹²⁾ on the other hand, is a deductive process. One assumes the occurrence of an event selected as the top, undesired event, constituting system failure. One then systematically works backward to identify component faults which could cause or contribute to the undesired event.

A complex web of events is involved in the uncontrolled release of radioactive material from a facility and the exposure of man. There are several points within the web at which one could define the initiating event for an event tree or the top, undesired event for a fault tree. These alternatives are illustrated in the next section.

4.2 THE WEB OF EVENTS

In Figure 2, a simplified diagram of the generalized web of events for facility release sequences facilitates comparing the methods reviewed for sequence identification. The figure is derived from a similar web for transportation accident release sequences.⁽¹³⁾ The points in Figure 2

FIGURE 2. A Simplified Diagram of the Generalized Web of Events for Analysis of Accidental Releases from Facilities

represent types of events, some of which are linked by lines to indicate a nonzero probability of occurring in the same release sequence. Time increases along the horizontal coordinate. The vertical coordinate provides a way to plot distinct types of events.

Across the top of the diagram are listed five general classifications of events, as they occur in a release sequence. Initiating events are typically those leading to exposure of the primary containment of the radioactive material to severe mechanical, thermal, and/or chemical environments. For example, a loss of cooling accident for water basin storage of encapsulated, solidified waste might involve power outage, pump failures, pipe failures, or various combinations of these.

Next are the types of events which actually negate the primary containment, resulting in release of radioactive material within the facility. Examples are waste canister failure or, for a liquid source, a vessel breach.

The events listed under Release from Facility are those which occur immediately following the failure of primary containment. They typically involve passage of radioactive material through various segments of the ventilation or offgas systems, culminating in exit from the building. Thus the first three categories involve events occurring almost exclusively within the facility.

The last two categories involve events which generally occur outside the facility. Events related to the environmental transport and deposition of the radioactive material are governed primarily by conditions such as weather and topography near the facility. Considerations such as land use factors lead into the final classification, Irradiation. This involves events of actual exposure, influenced chiefly by population density and radiological factors.

4.3 HOW VARIOUS SYSTEMS SAFETY METHODS HANDLE THE WEB OF EVENTS

Listed down the left side of Figure 2 are several ways of studying the release sequences. Model A is intended to indicate the total web of possible events. Models B, C, D and E indicate four ways of dividing the

problem into smaller pieces, to be followed by integrating the web back together so as to obtain the total result.

In Model B, which is intended to illustrate the event tree approach, one of the mutually exclusive initiating events (the point enclosed by the box in Model A) is followed along a widening path to the final events. For analysis of loss-of-cooling accidents, a pipe break might be selected as an initiating event.⁽⁷⁾

Model C is an attempt to depict a typical application of cause/consequence analysis. One of the mutually exclusive intermediate events, involving or preceding release of radioactive material from primary containment, is selected for study. All paths leading to this event, termed the "critical" event, are analyzed by fault tree analysis. The critical event is the top event of the fault tree. All subsequent events are handled as in the event tree analysis of Model B. The problem is neatly divided into two parts, the interface being the selected critical event.

If, in the example for Model B, a pipe break were the result of preceding, initiating events, then the analysis would probably be performed as in Model C. In both methods, the event tree branch probabilities are often obtained by means of separate fault trees. The top events of such fault trees are the branch events or decision points.

Model D represents the PNL fault tree technique. Each mutually exclusive, terminating point for A under Release from Facility is "clipped" or isolated. Events leading to each point are analyzed. Events proceeding from each point are analyzed. The two parts of the web are then rejoined to give the total flow of events.

In the application of Model D, the system fault tree is drawn with the top event representing release from the facility by any pathway. The mutually exclusive interface events described in the preceding paragraph are generally drawn as the next-to-top level events. They represent the various release modes out of the final containment barrier(s). Examples are airborne release up the stack, airborne release through the walls of the building, and release into a stream. The preceding events under Release from

Facility represent the flow of radioactive material through the ventilation and offgas systems of the facility. These events, as well as the primary containment failure events and the initiating events, all appear on the same fault tree. (A typical "to/through" fault tree appears in Appendix L.) Following the interface events, an event tree type of treatment is used to model environmental transport and deposition of the material and human exposure.

The prerelease (from the facility's outer barrier) events generally involve electrical, mechanical, and/or chemical events related to engineering. Postrelease events generally involve environmental and biological events falling in those scientific disciplines. If a complete set of mutually exclusive events (consisting of the release of certain types of radioactive materials in certain modes) is selected and the probability and radiological consequences of each type of release are calculated, then a value of risk can be estimated.

In Model E, one of the mutually exclusive final events is selected for study. All paths leading to it are studied by means of fault tree analysis.

4.4 SELECTION OF A SYSTEMS SAFETY METHOD

A potential weakness of any systems safety method exists in the process of uncoupling the web of events, performing independent calculations on these segments, then recoupling. Interactions among the uncoupled portions of the web are easily overlooked.

The approaches of Models B and C are vulnerable to interactions occurring within the facility.⁽¹⁴⁾ In Model C, the uncoupling occurs within the facility. In both Models B and C, the use of separate fault trees to develop the branch probabilities of the event tree could result in missed interactions between basic events in different fault trees. For example, a fire which fails the primary containment might also lead to failure of the ventilation system. Extreme caution is required in these methods to guard against missing such common cause failures.

An advantage of Model D over Model C is that in-facility events are treated on the same fault tree rather than on several fault trees and an

event tree. This tends toward a reduced possibility of overlooking in-facility common cause failures.⁽¹⁴⁾ The disadvantage is a more complex fault tree.

Model E may be the most rigorous model, at least on one point: in progressing from Model C to D to E, the top event of the fault tree comes closer to our ultimate interest--exposure of man. Also, Model E guards against undiscovered coupling between prerelease and postrelease events, to which the other models are vulnerable. Examples of such events are earthquakes, which could alter aquifers in the release area, and tornadoes, which could temporarily alter local meteorology. Unfortunately, Model E is generally too complex to be considered currently feasible.

Although there is disagreement among safety analysts on this point, we chose Model D over Models B and C for several reasons. It offers the more appealing logic and potentially greater thoroughness of working backward from an undesired event closer to the event of ultimate interest. Treating the facility as a whole, rather than uncoupling it into several subsystems, makes possible a more systematic defense against common cause failures. The approach eliminates the need to select a complete set of critical initiating or intermediate events. It also provides more compact graphic display for review by other safety analysts.

The authors are currently applying both event trees and cause/consequence analysis in safety studies of high-level liquid waste stored at a fuel reprocessing plant. In the Waste Fixation Program the same system is being analyzed by means of a fault tree, using the method described herein. Detailed comparisons of results obtained by means of the three methods are not yet complete. However, based on work to date, some tentative conclusions can be drawn. Fault tree analysis appears to provide more comprehensive identification of potential failure sequences. Furthermore, the computer techniques described herein are in place for calculating probabilities of large numbers (millions) of cut sets and for screening based on risk. Potential common cause failures of several safety systems are better displayed. On the other hand, event trees and cause-consequence analysis better facilitate and display the detailed analysis (particularly time-phasing) of accidents involving a common initiating or critical event.

Based on these preliminary conclusions, a fruitful combination of fault trees with the other two methods can be projected. A fault tree would be used as reported herein to provide the most comprehensive coverage of potential accidents and to separate those of prime interest. Detailed analysis of such classes of accidents could follow by means of event trees or cause-consequence analysis. Specialized techniques such as those discussed in Section 11 could be factored in.

4.5 SUMMARY OF THE TECHNIQUE SELECTED FOR CONSTRUCTING FAULT TREES

The particular technique selected for constructing fault trees, termed herein the "to/through" technique,* is similar to the leak path technique.^(15,16) Both depart somewhat from traditional ones for constructing fault trees. However, other investigators have already applied variations of this approach to safety studies of the following nuclear operations: generic fuel reprocessing plant, Fast Flux Test Facility, isotope separations/encapsulation plant, liquid waste storage, final storage of high-level waste, and transportation of plutonium.

Uncontrolled release of radioactive material from the system barriers, rather than failure of any one barrier or component, is postulated as the top, undesired event. This event constitutes system failure. Any sequence of events which could negate all pertinent containment/confinement barriers and result in occurrence of the top event is termed a release (or accident or failure) sequence. When such a sequence is identified on a fault tree and is treated mathematically by means of Boolean logic and probabilistic methods, it is often called a cut set.

All conceivable and physically meaningful combinations of events which could lead to release are systematically identified. (Because of the method's thoroughness, some sequences which are not physically meaningful

* The same terminology was applied earlier by Haasl⁽⁵⁾ in a more general sense. Fault tree analysis of electrical systems, for example, could be performed by considering the flow of electricity to a component and through the component. Because of the commonality of the thought processes in all such flow analyses, the name was retained.

may also be identified; of course such sequences must be discarded later.) The to/through method follows the flow of radioactive material in reverse sequence from its passage through the final barrier back to the initiating events that led to its flow through the initial barrier. The material must move to each barrier and pass through it for release to occur. One thereby investigates how each containment barrier could have been breached. The process is continued until initiating events have been reached (refer to Figure 2, Model D) and all conceivable release sequences of importance generated.

A simplified illustration of the to/through technique appears in Appendix A. A to/through fault tree from the Waste Fixation Program is shown in Appendix L.

The present technique of fault tree construction differs in other ways from those of many earlier fault tree analyses of nuclear systems. Near the bottom of the fault tree, component faults appear such as "pump fails to function" or "piping fails." These events are further developed not only into primary failures, but also into secondary failures (e.g., earthquakes, explosions), and command failures such as operator error and (where appropriate) nonfunction caused by power or other utility outage. In this manner, many potential common cause failures are displayed directly on the fault tree, rather than later being developed separately. For example, the possibility of several electrically powered components simultaneously failing to function because of a power outage can be studied. The simultaneous effects of a severe earthquake on several components within the facility can be examined. Use of different values of inhibit gate coefficients (also called⁽⁵⁾ constants of sensitivity) facilitates modeling differences in component earthquake resistance⁽⁴⁾ while retaining the common cause nature of the incident.

The present method emphasizes constructing the fault tree for a given operation as a complete entity. Some earlier studies apparently resulted in separate fault trees for different portions of a facility or for different processes in the facility. The present method improves treatment of possible dependencies among these subdivisions of the system.

Appendix B describes the PNL-developed ACORN code used for plotting fault trees for display purposes.

4.6 TREATMENT OF NONBINARY EVENTS

Fault trees are logic diagrams for portraying on-off behavior. That is, each event in the fault tree either occurs as described or it doesn't. This binary convention facilitates mathematical evaluation of the fault tree by Boolean algebra techniques.

The difficulties of modeling the behavior of real components in a binary fashion have been discussed.^(4,6,7) Binary techniques can best be applied to systems whose components either operate as specified or fail completely. These are faults which are of the on-off variety. However, many components can exhibit varying degrees of performance and can induce different accident sequences depending on their extent of failure. In such cases, strictly applying the binary logic requirements of fault tree analysis limits the accuracy of the modeling.

Unfortunately, little progress appears to have been made heretofore on this problem. Generally, one must either simplify the modeling of component behavior to fit the binary restriction or bend the restrictions of binary logic to fit the actual behavior of the system.

Sometimes, by carefully phrasing event descriptions, one can circumvent this problem. Examples are the descriptions "canister experiences a drop of ≥ 10 ft" and "valve fails to move $\geq 3/4$ full open." Results of this technique are often not completely satisfactory, however. One wonders for instance, what happens if the canister falls 9 ft (does it then have a zero probability of breach?) or if the valve sticks half open. Thus, partial failures still arise. They are still treated as complete failures or no failure at all. Depending on the shapes of the generalized stress/strength curves which describe component behavior, considerable error can result.⁽⁴⁾

This binary logic difficulty is of particular interest for a top event such as "uncontrolled release of radioactive material." One could phrase such an event as "release of $\geq x$ grams of radioactive material," inserting

an appropriate value of x . Such a description might be suitable for estimating the frequency of release $\geq x$ grams. However, the result would not indicate how much greater than x grams are the releases, so that the system risk might be estimated. A more serious difficulty with this technique was encountered when it was applied. Projecting release quantities upward from the basic events of the fault tree to the top, undesired event, so that the basic event probabilities corresponding to $\geq x$ grams (or between x and y grams) might be formulated, proved impractical with complex fault trees. The interactions were too complex and the number of cross-product terms (gross failure of one component coupled with minor failure of another, and vice versa) too numerous.

For handling this type of top event, the technique described below has proved far better. The top event is worded so as to include all off-normal releases of radioactive material, regardless of release quantity. (Normal releases may be either quite small or essentially zero, depending on the system. The first class would include a reprocessing plant; the second, transportation of nuclear materials.)

For identifying sequences, the binary behavior is retained and Boolean techniques are applied. That is, any off-normal release of radioactive material constitutes occurrence of the top event. As stated in Reference 7, "once a fault tree has been represented by its equivalent Boolean equations, it can then be evaluated by applying the laws of probability." The laws of probability allow application of many nonbinary mathematical tools. After identification, therefore, the probability and consequences of each cut set can be evaluated by whatever mathematical tools can be appropriately and consistently applied. See Reference 9 for the same type of discussion with regard to cause/consequence analysis.

The present technique allows each sequence to result in the release of a different quantity of radioactive material, as is the case with actual nuclear operations. This is facilitated by attaching either a single-valued or a distributed release fraction to each basic event in a sequence, as described in Section 7.6. (The distributed release fractions allow each sequence itself to exhibit a range of possible release quantities.) These

release fractions and the available inventory determine the release quantity for each sequence. The probability calculation is performed in the usual manner. Each release sequence is thereby characterized by a probability and a release quantity.

The result is that the sum of the probabilities of all release sequences (each of low probability) is a close upper bound⁽⁷⁾ to the total probability of the top event (release). And the information regarding the quantity released in each sequence is not lost. The probability of each sequence gives weighting information for its particular release quantity. Thus, a Farmer-type⁽¹⁷⁾ plot of release sequences, on axes of frequency or probability versus release quantity, is an almost direct extension from the results for the top event. Certain additional calculations of consequences are necessary. However, within a major branch of the tree (a term defined later), this would result only in a change of the release quantity scale to give an individual dose or a population dose. There would be no change in the ordering of the points representing the various release sequences.

4.7 CRITICAL REVIEW OF FAULT TREES AFTER THEIR CONSTRUCTION

The nuclear systems being analyzed are so complex that independent review of the fault trees is considered essential. The PNL review procedure is first to ensure that all failure sequences discussed in the SAR and other safety documents appear on the fault tree. Next, the tree is thoroughly reviewed by an independent in-house safety analyst. Operating personnel then check the fault tree against their knowledge of actual equipment and operating procedures. For conceptual systems, personnel most knowledgeable concerning the system characteristics are asked to examine the fault tree. Finally, fault tree consultants critique the tree.

THIS PAGE
WAS INTENTIONALLY
LEFT BLANK

5.0 SIMPLIFICATION OF THE ANALYSIS OF LARGE FAULT TREES

5.1 THE TASK OF ANALYZING LARGE FAULT TREES

The detailed fault tree modeling of systems, described in the preceding section, comes at the price of increased tree size and complexity. The Waste Fixation Program (WFP) fault trees were constructed by those procedures. The tree for water basin storage of solidified high level waste was found to include over 3.6 million Boolean-indicated cut sets (BICS).^{*} Each BICS represents a potential release sequence. The fault trees for liquid waste storage and for solidification of the liquid to a glass include about 7 million and 14 million BICS, respectively. Fault trees for more complex systems, such as a reprocessing plant, may be expected to include even more BICS.

It became obvious that detailed analysis of such numbers of cut sets was not feasible. Detailed analysis would require manual calculation of certain aspects of cut set behavior for which computerized procedures are unsuitable.

5.2 POSSIBLE SOLUTIONS TO THE PROBLEM

Possible solutions to the problem included the following: 1) since a complete, rigorous job cannot be done, abandon the effort; 2) do a thorough job on the portion of the operation or facility felt to represent the highest risk and omit the remainder; 3) do a superficial job on the entire system; i.e., construct a much simpler fault tree; 4) develop computerized techniques for performance of the detailed analysis which presently requires manual computations; 5) by approximate calculations, screen out the dominant (highest-risk) cut sets, then analyze them more thoroughly.

* As used here, a BICS is a set of basic events which can lead to occurrence of the top event. A BICS is not necessarily a minimal cut set. This is because of possible replication of basic events within a BICS and possible absorption among BICS. Furthermore, the number of BICS in a fault tree is greater than or equal to the number of minimal cut sets in the tree.

Alternative 1 provides no useful information. Alternative 2 is questionable because the one part of the system analyzed in detail may turn out not to be the process of highest risk. It would not be known how hazardous the other processes or portions of the facility are. Alternative 3 provides some information, but it may not be very reliable information. Simplified fault trees risk omission of important dependencies because of their limited degree of resolution. The authors are unaware of any sound methods for simple analyses of complex systems. Development of the computerized techniques for alternative 4 is not foreseen in the near future. The computer use charges for such techniques applied to large fault trees would undoubtedly be substantial.

Alternative 5 is clearly the most desirable.

5.3 DEVELOPMENT AND DEMONSTRATION OF A SCREENING METHOD

Efforts began in mid-CY-1974 to develop a suitable screening method. The resulting techniques enable one to rigorously identify and separate, based on a measure of risk (not simply probability), those sequences meriting more detailed study. An approximate risk sum of the discarded sequences is retained for later addition, giving the total calculated risk for the fault tree. See Figure 3. By facilitating early separation of dominant and of low-risk sequences, the screening process quickly identifies potential system weaknesses, controlling parameters, and R&D needs. This information is of particular interest for systems in the conceptual stage. A cost-effective approach requires this screening of failure sequences as early as it can be performed reliably. Detailed analysis of low-risk cut sets should be avoided.

About May, 1975, a successful screening and preliminary analysis was accomplished on a fault tree of more than 3.6 million BICS. The procedure has since been applied to other fault trees, including one with about 14 million BICS. Simultaneously, computer time requirements have been reduced. Fault trees with 1 million BICS can now be screened and preliminarily evaluated in typically 2 to 5 min of computer time on the Cyber 74. The tree with 14 million BICS required about 20 min.

FIGURE 3. Use of Preliminary Analysis, Screening, and Detailed Analysis to Obtain Total Calculated Risk for a System

The calculated risk of the cut sets which survive the screening (typically 50 to 5000 cut sets, depending on the size of the fault tree and the user's desires) has been found to represent nearly all of the risk for the entire fault tree. The value of this percentage, which varies significantly from one tree to another, cannot be determined exactly without completely analyzing the entire tree. However, a lower bound can be determined. This bound has ranged from 90% to 99+ % of the total risk in the tree.

The screening and preliminary evaluation method described here has proven quite versatile. It has been successfully applied to diverse fuel cycle operations. Included are transportation, liquid waste storage, water basin storage of solidified waste, solidification and canning operations, pipeline transfer operations between facilities, and Retrievable Surface Storage Facility operations. No unusual difficulties are foreseen in application to reprocessing or most other fuel cycle operations.

Some limitations are foreseen, however. 1) Applying any probabilistic method to studies of final storage is difficult because the extremely long time periods involved make probability assignment unreliable. 2) It is possible that reactor safety studies can be more readily done by means of event trees or cause/consequence analysis. This is because of the different physical processes and safety measures involved in potential reactor accidents (greater emphasis on heat transfer equipment, less emphasis on ventilation and offgas systems). Until a method like this one is used in a reactor safety study, no final judgment can be made. 3) The number of BICS that can be handled by the screening process is very large and is gradually being increased. However, situations arise in which this capacity is exceeded. In such cases, it is generally possible to recast the fault tree (as described in Section 7.3) to result in a much smaller number of BICS, with little or no loss of information. If this attempt fails, the recourse is to Monte Carlo techniques for fault tree analysis. However, such techniques "screen" based on probability alone; the present method screens based on probability multiplied by a measure of consequences. Only the latter method readily handles low-probability, high-consequence sequences. Personnel at PNL and elsewhere have studied the possibility of modifying Monte Carlo techniques to include consequences, but have had little success.

6.0 STATEMENT AND SIMPLIFICATION OF THE RISK EQUATION

6.1 BASIC CONSIDERATIONS IN SCREENING

Fault tree analysis has traditionally been used to calculate probabilities of event sequences leading to system failure. However, in nuclear risk analysis, the significance of a cut set is not measured solely by its probability. A second measure, the consequences, is also important. A cut set having a very low calculated probability might still represent significant risk if the consequences were quite large. Thus, screening of cut sets should not be performed on the basis of probability alone unless all cut sets so screened lead to similar consequences. In all other cases, the screening should be based on some measure of risk.

The fewer calculations required to ensure that a cut set represents insignificant risk (compared with that of other cut sets) and hence does not justify further analysis, the more efficient is the screening process. Various bases were studied for reaching this discard decision for individual cut sets or for large blocks of cut sets (major branches of the fault tree). Included were experience, intuition, and crude scoping calculations. Operating experience with the systems studied is seldom of sufficient magnitude or the data suitably organized to allow systematic decision-making. Use of intuition is difficult to defend and is not dependable. Crude scoping calculations can't be applied to millions of cut sets individually. Application to blocks of cut sets is possible if the probabilities and the consequences of one block outweigh those for a second block. However, such comparisons have seldom been found to be sufficiently clear cut to allow a decision when dealing with complex systems.

The present method includes use of scoping calculations to permit discarding large blocks of cut sets, but only if such discard decisions can be defended. For example, the risk represented by several smaller buildings at a reprocessing plant might be assumed negligible, based on scoping calculations, with respect to that represented by two or three of the main process and storage facilities. At best, however, such calculations have been found of limited value in screening. Other than for such limited contributions

from scoping, it was concluded that at least preliminary evaluation of all cut sets is needed to determine which cut sets contribute most to system risk.

The objective, then, was to develop a method for determining which cut sets constitute the highest risk (and, hopefully, the major portion of the risk), in terms of probability and consequences, and therefore justify more detailed examination. The only way identified to accomplish the screening was to actually calculate (or at least put an upper bound on) the risk, or a measure of risk, for each cut set in the fault tree.

6.2 STATING THE RISK EQUATION

For any cut set in a fault tree constructed as described previously, the calculated risk can be thought of as a mathematical product of five terms:*

$$R = A \times B \times C \times D \times E \quad (1)$$

where

A = probability of the release sequence;**

B = release quantity;

C = relevant measure(s) of the radioactive material characteristics (isotopic composition, size distribution, solubility, volatility, etc.);

D = a measure of environmental transport path efficiency;

E = a measure of population distribution, characteristics, and habits.

Equation 1 expresses risk as the product of probability A and consequences B x C x D x E. Other ways of expressing risk are discussed in Section 10.

* Throughout the report, expressions of risk or of risk measure are often written with the x symbol denoting multiplication (e.g., A x B, P x c). The aim is to emphasize the separate terms comprising the product. Elsewhere the x symbol is omitted, but the normal multiplication process is implied. For example, M (A x B)_{ref} is the product of M and (A x B)_{ref}.

** The release probability is denoted by A in discussions related to Equation 1 and to equations derived from it. In sections of the report which deal with probability calculation, the probability is denoted by P. The two symbols represent the same quantity.

The terms A, B, C, D, and E are used frequently in the rest of this report, with reference to their role in Equation 1. If appropriate quantities are attached to these five terms, Equation (1) can be treated as a strict mathematical product.⁽⁴⁾ Typical units of the five terms are, respectively, probability of an accidental release in a given time period, quantity released/accidental release, quantity of radiologically significant material dispersed/quantity released, quantity of radiologically significant material transported to man/quantity dispersed, individual or population dose/quantity transported to man.

A sixth term F, involving a conversion from dose to health effects,⁽⁴⁾ could be affixed to Equation 1. Still another term G, involving a conversion from health effects to a monetary measure, could be affixed, as in the proposed Appendix I of 10 CFR50 in the Federal Regulations.

The risk of a cut set is thus represented by the product of five types of parameters. Screening of cut sets could be done based on preliminary values for all five types of parameters. However, the labor would probably be prohibitive.

6.3 SIMPLIFICATION OF THE RISK EQUATION

6.3.1 Objective

Fortunately, for purposes only of comparing and screening sequences within a fault tree representing one facility at one site, we can simplify the risk equation. Judgment as to which of the following simplifications of Equation 1 can be made depends on the nature of the system and of the fault tree.

The following discussion shows how to group cut sets within a fault tree so that they can be screened simply on the value of the risk measure

$$R^* = A \times B. \quad (2)$$

Screening based on R^* is much faster than that based on the complete expression of risk R of Equation 1. (Typical units of R^* are grams or gallons

released in a year. In some cases, aspects of the C term may be included to give curies or measures more closely related to toxicity.)

6.3.2 Elimination of E (Population Factor)

For a fault tree representing a given facility or operation, differences in values of the E factor among cut sets are usually negligible. This implies that the population distribution, characteristics, and habits are independent of which cut set occurs. Thus, the E factor is generally not important in approximate comparisons of cut sets within a fault tree and may be omitted from the risk expression for purposes of screening. (A possible exception relates to population evacuation for some release sequences, but not for others. However, past safety analyses have generally assumed either no evacuation or evacuation independent of the release sequence. Another possible exception relates to transportation studies in which the population distribution might be different for different types of accidents. This case can be accommodated with minor modifications.)

6.3.3 Grouping on the Basis of D (Pathway Factor)

Site characteristics, such as weather, terrain, groundwater, surface water, and geology, control the D factor. Large differences often exist in the D factor for cut sets in the same fault tree. Failure sequences leading to groundwater transport may involve a D value orders of magnitude less than that for cut sets involving airborne release.

If the cut sets can be grouped by transport mode, however, cut set risks can be crudely compared within each group on the basis of $A \times B \times C$ calculations. Comparisons of cut sets in different groups are not valid without actual calculation of the various D factors.

A relatively small number (usually about five) of principal transport modes or, more precisely, general release classifications based on transport modes, are used. Examples are airborne ground level release, airborne elevated (stack) release, liquid under ground, or liquid into a stream. (Within each general release classification, radioactive material could reach

man via a large number of pathways.)⁽¹⁾ The number and identity of the general release classifications depend on the nuclear system, the source material present, and the site characteristics.

Each cut set must then be assigned to one of these general release classifications. Within a group (general release classification), the transport path efficiencies in carrying the material to man are very similar, and intragroup cut set comparisons are valid for screening purposes. For example, the airborne transport characteristics for release of x grams of material y at height z are generally independent of the in-facility failure sequence by which the material was released. In the great majority of cases, this is an excellent assumption. Exceptions such as tornado-caused releases have been mentioned in connection with Figure 2.

Classification of the cut sets by D group, that is, general release classification, has been found to be straightforward. Detailed identification of cut sets has not been found necessary. Examination of only the top two or three levels of a fault tree generally leads to one of the following conclusions: a) All cut sets in the tree involve the same, or similar, general release classifications, yielding identical or similar consequences per dispersible unit of a given material released. b) Several general release classifications exist, but the tree can be easily divided, at the second or third level from the tree top, into groups of cut sets exhibiting the same pathway behavior within each group. This is the more common case. For example, all cut sets under a given event near the top of the fault tree might involve elevated airborne release. (An important caution: there should be no AND gates above the point(s) on the fault tree at which cut sets are separated by D classification.)

Demonstration of the mathematical validity of the classification process is straightforward. The interpretation of the top event, as discussed in Section 4.6, is crucial to the argument.

Thus the fault tree is subdivided as necessary into major branches (an important term used frequently in following sections of this report) on the basis of general release classifications. Within each major branch, pathway

differences among cut sets can be neglected. Hence comparisons can be made on the basis of $A \times B \times C$ values.

Dominant cut sets in one D group can then be compared against those in another D group, if pathway differences (D factor) are included on at least an order-of-magnitude basis. Depending on the relative values of D for the various general release classifications, some groups of cut sets (major branches) may not justify more than scoping calculations of $A \times B \times C$. Groups of cut sets with an extremely low D value are generally not pursued. However, for each group, a trial calculation should generally be made for a few cut sets judged to be of highest $A \times B \times C$ value. The result should indicate whether to 1) discard the entire group as being of negligible risk compared with that in other major branches, 2) retain several cut sets within the group for further analysis; or 3) analyze the whole group. As mentioned previously, such discarding of entire major branches can only occasionally be defended. Of course, for all cut sets of high risk measure, detailed analysis of pathways and of population exposure is necessary after the sorting process.

6.3.4 Treatment of the C Term (Radioactive Material Characteristics)

The C term involves the physical, chemical, and radiological characteristics of the radioactive material. Several techniques may be used to treat this term for cut sets within a given D group, or major branch of the tree. The choice of technique depends on the radioactive material characteristics and on the types of accidents covered in the major branch.

One technique uses the fact that, within a D group, differences in C values from one cut set to another are often negligibly small compared with differences in $A \times B$ values. A simple example is provided by airborne release of particles from vitreous high-level waste following mechanical stress and containment failure. Here the C term may be defined as the quantity of transportable ($<10 \mu$ aerodynamic equivalent diameter, arbitrarily) fractured material divided by the total quantity of fractured material. Tests⁽¹⁸⁾ show that C, as defined, varies only about one order of magnitude from events of low mechanical severity to events of extremely high severity (117 fps impact against granite.) In fact, the variation with velocity is

less than that among specimens at identical velocities. Consider a major branch in which all cut sets involve airborne release following mechanical stress of waste glass of identical composition. Maximum differences in the C term from one cut set to another would be about one order of magnitude. Values of A x B terms commonly range over 10 to 15 orders of magnitude. Thus, in this case, cut sets can be screened based on A x B calculations only, if an allowance of one order of magnitude is made for the uncertainty in the C term. Figure 4 illustrates allowance for this uncertainty.

Likewise, the solubility of many forms of radioactive material is not highly dependent on the sequence of events which resulted in the exposure to water. There is an indirect effect of mechanical stress on surface area, but this might involve a range of only about two orders of magnitude.⁽¹⁸⁾ The implication of the uncertainty is that separations based on A x B can not be sharp, but must allow for possible overlap, as in Figure 4.

In other cases, the C term may vary significantly among a group of release sequences because an event appearing in some sequences but not in others changes the form or composition of the radioactive material released. Fires are an example of this class of events. The different volatilities of the various radionuclides in the material result in a postfire material of new composition. If the high-volatility elements are more toxic or are more readily transported to man, a higher dose results per unit of material released. Another event which might result in this fractionation of nuclides is passage through a selective filter.

Two techniques accommodate such situations. In one, the fault tree major branch is subdivided into subgroups. One subgroup might contain the sequences involving fire or meltdown; the other, the nonthermal sequences. However, in some cases, the tree structure may not be amenable to this subdivision process. The previous caution regarding AND gates again applies.

Generally it is advisable to use a technique in which the C term parameters of importance are included with the B term (quantity of material released). This is done as follows. The various radionuclides in the source term are compared on the basis of volatility, toxicity, filter DFs,

Case 1

Case 2

- Case 1. Cut set represented by top line clearly has risk measure less than that of cut set corresponding to bottom line. In fact, its risk measure is negligibly small by comparison, even if the uncertain C terms involved the worst combination of values.
- Case 2. It cannot be determined which cut set has greater risk measure because of the overlap of the uncertainty ranges. (Of course, with a more precise statistical treatment involving means and standard deviations, overlap would be allowed. It is the concept of data uncertainty, not the selection of statistical methods, which is of interest here.)

FIGURE 4. Illustration of the Effect of C-Term Uncertainties on Comparisons Based on Risk Measure $A \times B$ Only. (Length of line indicates uncertainties stemming from C term.)

transport efficiency, and any other pertinent parameters. The dominant radionuclide dose contributor for a unit release quantity is determined. The C term is then, in effect, combined with the B term. The composite term represents the quantity of the particular radionuclide which controls the dose, rather than the total quantity of radionuclides released.

For perspective, it should be noted that differences in C terms within a major branch have generally been found small. Separate calculations were made, first using RCG (Radiation Concentration Guide) data and then with actual airborne transport/dose modeling, for high-level waste. The results showed that cut sets with release quantities measured in terms of grams of finely divided ($1\ \mu$) material and cut sets with corresponding releases, measured in terms of grams of volatiles only, could appear in the same major branch and be screened effectively with resulting dose errors of generally less than one order of magnitude. Most release quantities themselves are not known that accurately. Compared with the very large differences in $A \times B$ products, the small C term differences should not materially affect the accuracy of the screening process. This is particularly true because sliding (not sharp) comparisons are made, as in Figure 4. Of course, the refined analysis phase, treating high-risk measure cut sets, must include more accurate treatment of the C terms.

6.3.5 Result

Within a major branch, representing all cut sets of a given general release classification, comparisons and screening can be performed on the basis of values of $A \times B$. (The C term must be handled by a technique such as those described previously, so that $A \times B$ comparisons are valid indicators of risk measure.) The units of this product are typically grams, gallons, curies or RCGs of radioactive material released per year. In some cases, the units may relate to a specific radionuclide rather than to the mixture of radioactive material in the original confined source.

The flexible procedures for simplifying the complete risk expression, $A \times B \times C \times D \times E$, to the risk measure, $A \times B$, for sorting comparisons has

been found widely applicable. However, careful judgment must be exercised regarding the validity of the C and E assumptions and the D classifications for each fault tree.

It is stressed that the screening and ranking process is intended only to simplify rigorously a large fault tree to a list of cut sets ordered on the basis of a risk measure. The principle illustrated in Figure 4 must be recalled in interpreting the ordered list. As shown in Figure 3, high ranking cut sets would be retained for further analysis.

7.0 PROCEDURE FOR SCREENING CUT SETS, BASED ON A x B VALUES

7.1 SELECTION OF SCREENING TECHNIQUE

Three techniques were considered for performing the screening and ranking process: use of manual evaluation, Monte Carlo fault tree codes, and analytical fault tree codes.

7.1.1 Manual Evaluation

Fault trees which are sufficiently simple can be evaluated by hand. This was done with the relatively small tree for the WFP Retrievable Surface Storage Facility, Sealed Storage Cask Concept, as a checkout of procedures later computerized. Obviously, few fault trees representing nuclear operations are amenable to hand calculations without considerable simplification. Another drawback is the high probability of committing errors in manual calculations.⁽¹⁹⁾ Advantages include its flexibility and the visibility provided of the calculations being performed. For these reasons much of the detailed analysis phase is performed manually. However, the method is not well suited for screening large fault trees.

7.1.2 Monte Carlo Fault Tree Codes

An example of this type of code is SAFTAC.^(20,21) Such codes are designed to calculate failure frequencies of systems, i.e., the A term of the A x B product. Indeed, truly enormous fault trees can be analyzed on this basis by Monte Carlo codes. However, difficulties are encountered in adapting such codes to simultaneously calculate both probability and consequences. Without such adaptation, cut sets of extremely low probability yet high consequences may never appear as output within a reasonable amount of computer time. This problem was also encountered by VanSlyke⁽²²⁾ in risk studies of waste storage tanks.

A code such as SAFTAC could be run once for each of several values of B (release quantity). Each B value would have an associated value of probability for each basic event. As discussed in Section 4.6, application of this scheme had little success.

7.1.3 Analytical Fault Tree Codes

The analytical techniques of fault tree analysis result, in theory, in the identification and evaluation of every minimal cut set in a fault tree. As noted previously, Monte Carlo techniques identify and evaluate only those cut sets which appear as output within the number of system simulation periods performed. Because the analytical approach had the potential to overcome the disadvantages of the previous techniques, it was selected.

Several analytical fault tree codes were available in mid-1974. However, it was concluded that none was capable of identifying and preliminarily evaluating all cut sets of very large fault trees in reasonable amounts of computer time. VanSlyke⁽²²⁾ reached the same conclusion. Extensive modification of a recently published code⁽²³⁾ led to two PNL codes (FAULT and FAULTG) capable of implementing the screening method.

Details of the fault tree analysis and screening procedure developed and its advantages and disadvantages are given in Sections 7.4 through 7.7 and in several appendices. A summary of the procedure follows immediately.

7.2 SUMMARY OF THE SCREENING PROCEDURE

The computerized screening procedure involves use of an analytical fault tree code (FAULT or FAULTG) to conduct successive screenings of cut sets, based sequentially on application of 1) a derived cutoff, n_{cut} , for the maximum number of unique basic events in a cut set (all cut sets with at least this number of basic events are discarded from further analysis, but are retained for estimating total risk) and 2) a derived cutoff, A_{cut} , for the minimum probability of a cut set. Probabilities (A terms) are calculated, based on extensions of Reference 7 equations, for all cut sets or event chains surviving the first cutoff. These probabilities are compared with the probability cutoff. Cut sets with probabilities below the cutoff value are discarded from detailed analysis, but are retained for estimation of total risk.

For all cut sets surviving this second cutoff, values of release fractions and total available inventory are attached to give an approximate value of the B term (release quantity). The release quantity is multiplied by the probability to give a value of $A \times B$ for each cut set. The cut sets are then ranked in order of their values for the $A \times B$ product. All of these B and $A \times B$ calculations are performed by code RAFT. The result is an ordered list of important cut sets, based on preliminary values of the risk measure $A \times B$. Such top-ranking cut sets are logical candidates for more detailed study.

The summation of $A \times B$ products for the higher ranking cut sets is calculated. Separately, the summation of $A \times B$ products for cut sets discarded in the screening process is also estimated. This is done because a very large number of cut sets, each of extremely small risk, could represent a significant contribution to system risk. This separate summation (discussed in Section 8.2), combined with the sum of the risk measures of the most important cut sets, gives the total risk measure for all cut sets in the major branch of the fault tree. This was shown in Figure 3.

Figure 5 describes how the screening process leads to the separation of high-risk and low-risk sequences for a major branch. This process corresponds to the upper portion of Figure 3. The roles played by the various computer codes are indicated. Figure 6 shows the effect of the screening process on the overall risk analysis calculational flow of Figure 1.

7.3 PRELIMINARY SIMPLIFICATION OF FAULT TREES

Before the screening procedure is discussed in detail, it is noted that the labor of evaluation can be reduced, with little loss of accuracy, by following certain tree construction guidelines. Examples are minimizing the use of on-off switches and limiting the number of inputs to logical OR gates by means of hand-calculated comparisons of inputs. Additional guidelines,

FIGURE 5. Schematic of Screening Process for a Major Branch. The risk sum of all discarded sequences is estimated for later addition to give the total risk in the entire fault tree.

FIGURE 6. Effect of Screening Process on Risk Analysis Calculational Flow. Compare with Figure 1.

which can result in greater reduction, have been discussed by Pande et al.⁽²³⁾ In one example therein, the revisions reduced the number of BICS by three orders of magnitude with no loss of accuracy because only repeated cut sets were eliminated. Similar and even more extreme cases have been observed at PNL. For example, a tree was reduced from 56 million to 3 million BICS by recasting a small, repeated section according to the guidelines. In another case the number of BICS was reduced from $>10^{15}$ to 10^7 . No loss of information resulted because the omitted cut sets represented either replications of other cut sets or impossible sequences.

These guidelines may be applied before submitting the fault tree to screening, especially if an extremely large tree is involved. Alternatively, recasting may be restricted to only those trees for which the screening process lacks sufficient computer capability. The PNL fault tree evaluation codes include a feature for counting BICS as a function of their length before analysis of the fault tree.

7.4 DERIVATION OF THE CUTOFF VALUES

7.4.1 Selection of a Reference Cut Set

If the $A \times B$ product can be manually evaluated for one simple cut set, called the "reference cut set," in the branch of the tree under study, then a cutoff scheme can be formulated. (In general, a different reference cut set is required for each major branch.) Only cut sets whose $A \times B$ products are not negligible compared with that of the reference cut set, $(A \times B)_{\text{ref}}$, would be retained for further study. The closer the $A \times B$ value for the reference cut set is to that of the cut set with the highest risk measure, the more efficient will be the screening.

The $(A \times B)_{\text{ref}}$ value could also be selected arbitrarily, but use of the reference cut set concept is more appealing and more reliable. Use of an arbitrary $A \times B$ cutoff value, as such, is discouraged, an ordering of cut sets on the basis of $A \times B$ values being sufficient. However, the concept of an $A \times B$ cutoff, based on $(A \times B)_{\text{ref}}$, is helpful in deriving defensible values of the cutoffs for probability and for event chain length. These derivations are discussed in 7.4.2 and 7.4.3.

The reference cut set is selected based on its ease of evaluation and on a judgment that its risk measure is among the highest in the major branch, so as to maximize screening efficiency. The type of cut set selected depends on the system under study. For highly passive nuclear systems it may involve events such as earthquakes or aircraft strikes. For nuclear systems with a larger number of active components, it may involve the events previously mentioned or events such as cooling system failures. Events such as aircraft strikes are usually good choices for this purpose because approximate analyses are not difficult to perform and because such events often represent a non-negligible fraction of system risk.

The reliability of the screening procedure is not adversely affected if a reference cut set is selected whose $A \times B$ value is not among the higher values in the major branch. If a cut set having a lower value of $A \times B$ is selected, the screening will simply be less efficient because a number of cut sets of low risk measure will unnecessarily be carried along for $A \times B$ ranking. This will be evident from the initial computer output. The value of $(A \times B)_{\text{ref}}$ can be readjusted upward and the screening repeated. In applications to date involving fault trees for various nuclear operations, no difficulty has been experienced in this regard.

If $(A \times B)_{\text{ref}}$ is mistakenly set too high (at a value to which no cut set corresponds), the screening will be "too efficient" in the sense that important cut sets will be omitted. For example, if $(A \times B)_{\text{ref}}$ were arbitrarily chosen rather than being based on an actual cut set, perhaps no cut sets would survive the screening. Since cut sets are selected for further study based on $A \times B$ ordering, no irreversible loss of information would result. The scarcity of cut sets surviving the screening would merely indicate that the screening should be performed again with a lower value of $(A \times B)_{\text{ref}}$. The use of derived, rather than arbitrary, cutoffs is recommended in order to minimize the possibility of this sort of difficulty. Some trial and error may be necessary with this aspect of the screening procedure, although none has been necessary in applications to date. Important quantities to observe are the number of cut sets surviving the screening and the distribution of their $A \times B$ values.

The concept of a reference cut set and of cutoff values for probability and chain length used in screening are not in any way intended to represent judgments regarding acceptable or unacceptable levels of risk or probability. They merely serve as very flexible tools in the screening and ordering procedure.

7.4.2 Probability Cutoff

The probability cutoff, A_{cut} , is assigned by solving the equation

$$A_{\text{cut}} \times B_{\text{max}} = M (A \times B)_{\text{ref}} \quad (3)$$

Here B_{max} is the maximum conceivable quantity of radioactive material which could be released from the system for any release sequence in the major branch, M is a multiplicative constant (generally arbitrarily set at 10^{-3} to 10^{-4}), and $(A \times B)_{\text{ref}}$ is the $A \times B$ product of the reference cut set described previously.

Equation (3) shows that the risk measure of any cut set (in the major branch) with probability $A \leq A_{\text{cut}}$ is negligible, compared with the risk measure of the reference cut set, by a factor of $\leq M$. Even if the release quantity associated with the cut set were the maximum conceivable value, the risk measure would still be negligible compared with that of the reference cut set. This screening reduces the need for calculation of release quantities (the B term) for cut sets which would be discarded later anyway, thereby greatly reducing calculational effort.

For the WFP water basin storage fault tree, a typical calculation is shown below.

$$A_{\text{cut}} = \frac{M (A \times B)_{\text{ref}}}{B_{\text{max}}} = \frac{(3 \times 10^{-3}) (10^{-1}) \text{g}}{(1.3 \times 10^7) \text{g}} = 2.3 \times 10^{-11} \text{ yr}^{-1},$$

where $M = 3 \times 10^{-3}$ and $B_{\text{max}} = 1.3 \times 10^7 \text{ g}$. Cut sets of probability $\leq 2.3 \times 10^{-11} \text{ yr}^{-1}$ would not be retained for detailed calculations. (However, the risk sum of such low-risk cut sets would be estimated as shown in Figure 3.)

The M factor includes several considerations. First, it provides a measure of negligibility in cut set comparisons. In approximate comparisons for risk analyses, one quantity may often be said to be negligible with respect to a second quantity if their ratio is smaller than 10^{-1} or 10^{-2} . The M factor also allows for the uncertainties in the quantities being compared, as illustrated in Figure 4. Only if the uncertainty bands do not overlap can a discard decision be made (unless more precise statistical treatments are used). Uncertainties in A and B, as well as in C, should be considered in establishing the value of M. The wider the uncertainty bands of the A x B products, the larger the negative exponent of M. Values of 10^{-4} for M are typical, representing factors of 10^{-1} for negligibility and 10^{-3} for uncertainty.

7.4.3 Event Chain Length Cutoff

If one could reliably determine, essentially by inspection rather than by calculation, that most cut sets in a major branch could not result in probability values $A > A_{\text{cut}}$, much computer time could be saved. Calculation of A values would not be necessary for such cut sets. It might not even be necessary to fully identify the cut sets. Such a procedure exists through the concept of a cutoff on the length of the release sequence chain--the number of unique basic events comprising a cut set.

7.4.3.1 General Approach

Chain length cutoffs have been used in previous fault tree analyses, but the cutoff criteria were such that results were not completely dependable. In one instance, the chain length cutoff was chosen arbitrarily. In another, the cutoff was based on the number of active and passive components represented in a cut set. The present derivation is considered more rigorous.

For a cut set composed of n unique basic events, an upper bound as a function of n, $A_{\text{ub}}(n)$, can be placed on the cut set probability, A. This can be done by conservatively assuming that the n highest probability basic events in the major branch compose a single cut set. (In reality, these n events may never appear together in any one cut set.) By formulating a

sequence of upper bounds, $A_{ub}(1)$, $A_{ub}(2)$, ... for cut sets of 1, 2, ... events, respectively, one can determine the minimum number of events, n_{cut} , for which $A_{ub}(n_{cut}) \leq A_{cut}$. All cut sets with $\geq n_{cut}$ terms will have probability values $A \leq A_{cut}$ and need not be retained for detailed calculations. This is evident because, for every n , $A(n)$ for every cut set is $\leq A_{ub}(n)$.

The need to calculate the actual A values for such cut sets is eliminated. Identification of all events in such cut sets is not even necessary. One merely ensures that a partially identified cut set (e.g., $X_1 X_2 X_3 E_1$) consists of at least n_{cut} unique basic events X , plus any number of non-basic events E . For example, if $n_{cut} = 10$ and a cut set has an unknown value of $n \geq 10$, then the cut set can be discarded, even though it is not totally identified at this stage. (A subtlety regarding absorption is discussed in Appendix E.) A considerable saving in computer time results from use of the cutoff on cut set length.

7.4.3.2 Calculation of the Cutoff on Event Chain Length

Equations for rigorously determining n_{cut} , the cutoff for the number of unique basic events (including inhibit gates) in a cut set, are derived in Appendix D. The basic types of cut sets which can be accommodated include nonrepairable components only, repairable components only, mixtures of these types of components, and cut sets including inhibit gates or switches. Schemes to obtain the sequence of upper bounds, $A_{ub}(1)$, $A_{ub}(2)$, ..., are given. The closer the upper bounds are to the least upper bounds (the highest actual $A(n)$ values in the major branch), the more effective is the screening. However, upper bounds of high accuracy require lengthy manual calculations. An optimum combination exists for the total expense of manual and computer time.

The method for determining n_{cut} involves the probabilities P_i and unavailabilities Q_i for all basic events i in the major branch. Consequently, the value of n_{cut} varies from one fault tree to another. It also may vary from one major branch to another within the same tree, depending on which basic events appear in each major branch. Only a nonarbitrary method for determining n_{cut} has the flexibility to accommodate the characteristics of various nuclear operations.

An actual application of the n_{cut} method is shown in Appendix D. For a preliminary fault tree involving water basin storage of solidified high-level waste, $n_{\text{cut}} = 10$. Thus, all cut sets of ≥ 10 unique terms may be discarded.

The following simplified example also illustrates the derivation of the cutoff. Assume a fault tree has only the basic events X_1, X_2, X_3, X_4, X_5 , (all nonrepairable), with probabilities of $10^{-5}, 10^{-4}, 10^{-6}, 10^{-7}$, and 10^{-3} , respectively. Assume $A_{\text{cut}} = 2.3 \times 10^{-11}$. The most probable two-event cut set is $X_2 X_5$. Its probability is the product of 10^{-4} and 10^{-3} , or 10^{-7} , a value greater than A_{cut} . Thus, all two-event cut sets must be retained at this stage. The most probable three-event cut set is $X_1 X_2 X_5$. Its probability is 10^{-12} , which is smaller than A_{cut} . Thus, all three-event cut sets can be eliminated from detailed analysis.

7.4.3.3 Savings Achievable by Use of an Event Chain Length Cutoff

Figure 7 shows the number of cut sets and their distribution as a function of n , the number of basic events (including inhibit gates) per cut set, for several preliminary WFP fault trees. All distributions except that for the water basin represent minimal cut sets actually identified. The number of BICS (about 56 million) in that tree was calculated by means of an algorithm in code FAULT. The algorithm does not account for repeated events within a cut set nor for repeated cut sets. Thus the curve of cut sets (rather than BICS) would shift somewhat to the left and downward. The location of the cutoff on n is shown for the water basin tree.

The curves have considerable central tendency (they are plotted logarithmically) and some skewness. Distribution peaks occur at a little more than half the maximum length of cut sets.

The event chain length cutoff is the first screening for reduction of the number of cut sets. Figure 8 illustrates the effectiveness of this cutoff. The accumulated percentage of cut sets having $\leq n$ events is plotted against n . For the water basin tree, only 2% of the BICS have ≤ 9 events. For this tree, only cut sets of ≤ 9 events need be retained (Appendix D), so the work is reduced by a factor of about 50 as a result of this cutoff alone.

FIGURE 7. Distribution of Cut Set Lengths in Several Preliminary Fault Trees

FIGURE 8. Accumulation Curves of Cut Set Lengths for Several Preliminary Fault Trees

The factor of reduction due to n_{cut} varies widely, depending on the fault tree construction and on the P_i (probability) and Q_i (unavailability) values for the basic events in the branch. Although factors considerably higher than 50 are probably attainable, the above example represents a better than usual result. Factors as low as 3 have been observed. In such cases, the bulk of the screening effort falls upon the probability cutoff A_{cut} . Reduction factors ranging from 100 to 8000 often result from applying A_{cut} to large fault trees.

7.5 HANDLING THE A TERM: CUT SET IDENTIFICATION, PROBABILITY CALCULATION, AND SCREENING

Codes FAULT and FAULTG have been developed by PNL to identify the cut sets in a major branch, to calculate their probabilities, and to screen them by means of cutoffs n_{cut} and A_{cut} . Although either code (or the ALLCUTS⁽²²⁾ code) can be used for these purposes, FAULTG, a revised version of FAULT, has exhibited the shortest running times.

7.5.1 Code FAULT

FAULT derives from the TREEL-MOCUS code,^(23,24) used for identification of cut sets. The basic input/output formats and the MOCUS algorithm for identifying cut sets were retained. The algorithm to find the minimal cut sets from the complete list of cut sets (BICS) was deleted for reasons stated in Appendix E. Extensive changes were made in order to 1) greatly increase the code capacity, 2) add the capability of calculating cut set probability, 3) incorporate the screening procedure, and 4) account for cut set disposition.

7.5.1.1 General Function

Input to FAULT includes the fault tree logic and the event descriptions, data for component failure probability and unavailability, and cutoff values for cut set length and probability. See Figure 5.

FAULT consists of three main sections. The first transforms the input tree logic into an ordered form for further analysis and performs error checking. The second section is the algorithm to identify the individual

cut sets in this ordered tree, starting from the top, and to perform the specified degree of Boolean reduction. If an undeveloped cut set accumulates n_{cut} unique events, it is discarded. Large numbers of cut sets are thereby eliminated at a single decision point, saving much computer time.

In the third section of the code, probability calculations are made, using the equations of Appendix C, for each fully developed cut set as it is identified. The cut set is discarded if its probability is below the probability cutoff A_{cut} . This operation continues until the last cut set string has been processed and all basic events encountered. All cut sets of interest will then have been determined. Surviving cut sets and their probabilities are ordered and are printed and/or put onto file for future input to the RAFT code (described in Appendix G). See again Figure 5.

In conjunction with these functions, FAULT has several options. These include 1) an algorithm to estimate the number of BICS versus the number of events per BICS; 2) the capability of reading in the complete fault tree and then specifying any gate as the top gate to analyze; 3) the option of using a probability cutoff; 4) the option of using a cutoff on the number of unique events per cut set; 5) recording the disposition of the cut sets in the use of the cutoffs; 6) the option of ordering cut sets by size; 7) the option of printing cut sets and/or creating a file for further processing.

As previously stated, complete absorption to minimal cut sets is bypassed. However, FAULT does perform the necessary Boolean reduction for repeated events within a cut set. It also checks for repeated cut sets at each substitution point and eliminates them as found. Since the cut set identification algorithm works downward, only a complete comparison of all the stored cut sets can eliminate all repeated cut sets. This check is time consuming; consequently, code RAFT, which uses FAULT output, performs a complete check for repeated cut sets.

FAULT operation is further discussed in the next subsections. Detailed input/output information appears in Appendix F.

7.5.1.2 Code Capacity

The code's capacity was greatly increased by use of disk scratch files rather than use of core only. Fault tree major branches with several million BICS have been successfully analyzed in a few minutes of computer time. The present storage configuration limits the number of cut sets (in a major branch) surviving both cutoffs to about 400,000. Use of tape storage files would again increase the capacity considerably. However, a more than proportional increase in running time would result because of less efficient operation.

7.5.1.3 Probability Calculations

PNL-developed equations (discussed in Appendix C), based largely on those of Reference 7, have been added for simplified calculation of cut set probabilities. The assumptions of small probabilities and of constant failure rates are made. More sophisticated equations could be used, but, in general, the lack of data and the looseness of the problem description do not justify the effort. The equations accommodate AND gates, OR gates, inhibit gates, and on switches (houses) and off switches. Cut sets can consist of repairable components only, nonrepairable components only, or mixtures of both types. Components can be online or standby. Unavailability contributions from pre-existing failures, failures on demand, and testing and maintenance downtime can be handled. Manipulation of the equations to produce an easily programmable form is demonstrated in Appendix C. Several sample calculations for cut sets of various mixtures of component types are given.

7.5.1.4 Cut Set Accounting Procedures

Routines have been added to the code to give detailed information about the initial size of the fault tree and the effectiveness of the screening. This information provides valuable insights into the course followed by the code in the screening process.

An improvement has been made in the routine (derived in Reference 25) which counts the BICS in a tree prior to analysis and screening. The results are now given as a table of BICS length versus the number of BICS of

that length. Being based on BICS, this information includes duplicate cut sets as well as cut sets with repeated events. However, the table helps scope the size of the fault tree analysis problem before proceeding. Based on the table of results, strategy can be developed or altered without committing large amounts of computer time.

Cut set disposition resulting from screening is also recorded. The numbers of cut sets discarded due to the cutoffs on event chain length and on probability are recorded. The number of discarded duplicate cut sets is also given.

7.5.2 Code FAULTG

Code FAULTG is a revised version of FAULT, identical in aims. The three basic functional sections described previously are used. FAULTG uses the same probability equations as FAULT and can accommodate the same gate types.

Although developed independently, FAULTG is based on the same type of upward-working algorithm for cut set identification used in the MICSUP code.⁽²³⁾ The MICSUP algorithm has been described by Chatterjee.⁽²⁵⁾ By dealing only with basic events, these codes eliminate repeated calculation of the same cut sets.⁽²⁵⁾ The cut sets for an intermediate gate in the tree can be given without further processing. The biggest improvements over MOCUS-based codes such as TREEL-MOCUS and FAULT, however, are in shorter computer time and reduced storage requirements.

FAULTG processes first those gates having only basic event inputs. As the code processes each gate on its way to the top event, checks are made 1) for all duplicate cut sets, 2) of cut set length against n_{cut} , and 3) of the calculated cut set probability against A_{cut} . Each surviving cut set, along with its gate, is stored on disk for use in upper levels of the tree. These steps are repeated until the top of the tree is reached.

The code eliminates a gate and its cut sets from mass storage when the gate is no longer needed, thus resulting in efficient mass storage usage.

Once the specified top of the tree is reached, the cut sets are printed and a file is created for input into RAFT. Running time is greatly reduced because duplicate cut sets and cut sets not surviving the cutoffs are discarded low in the tree and undergo no unneeded processing. A gate need be evaluated only once using the upward algorithm of FAULTG. The downward algorithm in FAULT evaluates the same gate many times. Limited experience to date indicates approximately an order of magnitude reduction in computer time for FAULTG, compared with FAULT, on large fault trees.

FAULTG, also, is limited to about 400,000 cut sets surviving both cutoffs.

FAULTG has features and options very similar (but not identical) to FAULT, including the following: 1) an algorithm to estimate the number of BICS versus the number of events per BICS; 2) the capability of reading in the complete fault tree and then specifying any gate as the top gate to analyze; 3) the option of using a probability cutoff; 4) the option of using a cutoff on the number of events per cut set; 5) the option of recording the disposition of cut sets at each gate; 6) the option of printing cut sets; 7) the option of creating a file of cut sets discarded at the top gate; 8) the option of checking for redundancy of cut sets. (FAULTG automatically checks for repeated events within a cut set and performs the necessary Boolean reduction.)

Detailed input/output information appears in Appendix F.

7.5.3 Probability Data

Sources of information for assigning basic event probability and unavailability are 1) experience with the component or a similar component, 2) testing of full-scale and subscale hardware, 3) engineering analysis, and 4) engineering judgment, including relative weighting and allocation. Many events require probability assignment by engineering judgment because of the lack of operating experience, test information, and analysis.

A detailed discussion of specific data or data sources is beyond the scope of this methods report. Much of the available data appropriate for

nuclear operations has been compiled in Reference 7. Other compilations exist, as do computerized data banks.

7.6 HANDLING THE B TERM (RELEASE QUANTITY) AND THE A X B PRODUCT

7.6.1 Introduction and Summary

The risk measure used for screening is the A x B product. This quantity represents the release sequence probability multiplied by the quantity of radioactive material released from all containment barriers. The first term is calculated by code FAULT or FAULTG. (See Section 7.5 and Appendix F.)

Calculation of the B term and of the A x B product is performed by the PNL code RAFT, whose input/output description appears in Appendix G. RAFT receives information from FAULT or FAULTG regarding all cut sets surviving the cutoffs on event chain length and cut set probability. Duplicate cut sets are removed by a scheme for rapid redundancy checking. The B term is calculated for each remaining cut set. (Normalization, discussed in 6.3.4, may be needed to account for the C term.) Each B term is multiplied by its corresponding A term (from FAULT or FAULTG output), giving the A x B products. The cut sets are then ordered on the basis of this product.

The fractional contribution of each set to the total risk measure of all cut sets handled by RAFT is given, along with the value of that total risk measure. As an option, an estimate of the risk measure sum of the discarded sequences is calculated (see Section 8.2).

7.6.2 Calculation of A x B Products by Code RAFT

Code RAFT reads the list of surviving cut sets and the probability for each from FAULT or FAULTG output. User input to RAFT includes values of the release fractions for all basic events and the total inventory available. See Figure 5.

7.6.2.1 Release Fractions

Each basic event, including inhibit gates and switches, is assigned a value for the release fraction. This term is defined as the amount of radioactive material available at the output or completion of the event divided

by the amount available at the input or beginning of the event. The release fraction is essentially the inverse of the widely used DF (decontamination factor) parameter.

Some basic events do not have a physically associated release fraction. Examples are the events "fan fails," "failure of primary electric power," "water supply unavailable." Such events, for which the release fraction is set equal to 1.0, have no direct effect on the overall release fraction of sequences in which they appear.

Most basic events are assigned a single-valued release fraction, whose value is less than or equal to 1.0. Other basic events, especially those related to failure of critical containment/confinement barriers, may be assigned distributed release fractions. This freedom facilitates treatment of a "spectrum problem": even for a given failure mode, not all failures of a given component involve the same release fraction.^(4, 26-28) Examples are failures of HEPA filters, of spray systems for removing airborne contamination, and of components of offgas systems. Such a basic event, X_j , would be modeled as having RF_{j_1} (release fraction number one) at CP_{j_1} (conditional probability number one), RF_{j_2} at CP_{j_2} , ..., RF_{j_L} at CP_{j_L} . The condition $\sum_{i=1}^L CP_{j_i} = 1.0$ must hold. Currently, code RAFT limits L to a maximum value of 4. The accuracy of existing data seldom justifies finer resolution.

Distributed release fractions can be assigned to all basic events with $RF \neq 0$ in the major branch. Again, the accuracy of available data seldom justifies its use for more than a few basic events. Furthermore, greatly increased computer time for RAFT would result.

7.6.2.2 Total Available Inventory

The other input quantity for RAFT is the total inventory available (TIA) of radioactive material. This quantity is often identical for all cut sets within a major branch. Then only one number is required.

If several potential sources are represented on the major branch, the TIA value may differ for different cut sets. This situation is handled by modifying the release fractions associated with failure of the initial containment layer(s) for such sources, in the following manner. The largest potential source is assigned the TIA input to RAFT. Release fractions associated with the initial containment barriers for the other potential sources are multiplied by a correction factor. This factor is the ratio of the magnitude of the source of interest to that of the largest source of interest. Depending on the source material and the analyst's preferences, weighting by some measure of potential toxicity, as well as by volume or mass or curies, may be included in the ratio.

7.6.2.3 Calculational Procedure

The procedure for calculating $A \times B$ is given below for several cases of release fraction input. A cut set consisting of basic events $X_1, X_2, \dots, X_n$ and having probability A is assumed.

Case 1 There are no distributed release fractions for events in the cut set. The release fractions are RF_1 for X_1 , RF_2 for $X_2, \dots, RF_n$ for X_n .
 $B = (TIA) RF_1 RF_2 \dots RF_n$
 $A \times B = A (TIA) RF_1 RF_2 \dots RF_n$
 For each cut set of this type, only one additive $A \times B$ term arises.

Case 2 Basic event X_j has a distributed release fraction. All remaining basic events in the cut set have single release fractions as before.

If the release fraction distribution for X_j has L pairs of (RF_{j_i}, CP_{j_i}) values, then $A \times B$ for the cut set consists of L additive terms (sub-cut sets):

Term 1 yields $(A)(CP_{j_1})(TIA)RF_1 RF_2 \dots RF_{j_1} \dots RF_n$

Term 2 yields $(A)(CP_{j_2})(TIA)RF_1 RF_2 \dots RF_{j_2} \dots RF_n$

⋮

Term L yields $(A)(CP_{j_L})(TIA)RF_1 RF_2 \dots RF_{j_L} \dots RF_n$.

These L contributors constitute the total $A \times B$ product for the cut set. Code RAFT prints a record of (up to 37 per cut set) the

contributors of highest magnitude, including the values of probability and release quantity as calculated by the above equations. This information indicates which part of the release fraction distribution contributes most to the calculated risk measure. Further analysis or testing in that region may be advisable.

Case 3 Several basic events in the cut set have distributed release fractions. This is the most general case.

Assume m basic events have distributed release fractions, with one distribution having L_1 values, another having L_2 values, and the m^{th} such basic event having L_m values. Then the $A \times B$ product for this cut set consists of $L_1 L_2 \dots L_m$ additive contributions (sub-cut sets). The technique in Case 2 is readily extended to accommodate Case 3. The technique includes treatment of the cross-product terms resulting from multiple distributions.

7.6.3 Difficulties in Assigning Release Fractions

Release fractions have long been a difficult area of nuclear safety analysis. Aside from the problem of obtaining adequate data, other difficulties arise in treating release fractions in connection with fault trees. These difficulties, and schemes for handling them, are discussed below.

It is sometimes hard to select the basic event to which a given release fraction can most accurately be applied. Much more is involved than merely listing basic events and attaching release fractions. Only a detailed examination of the fault tree, considering which failure sequences contain which basic events, can prevent the double application or the omission of release fractions. For handling secondary failures, it has generally been found most convenient to assign the release fractions to the inhibit conditions.

Particular care must be taken in assigning release fractions to basic events in transferred portions (using the standard triangle symbol) of the fault tree. Sometimes, in the transferred location, the event has a slightly different significance because of different events appearing with it in the same cut set. The original release fraction may no longer be

appropriate. If the point of transfer is located in a different major branch of the tree, no difficulty results because separate computer runs would be necessary anyway. If the transfer is within the same major branch, at least two possible solutions exist: 1) apply a modifying factor to release fractions of other basic events in the cut set so that the overall release fraction assumes the desired value; 2) add a dummy inhibit condition, such as "release path present," to achieve the desired change in release fraction.

Another difficulty, related to the preceding, is that a basic event may exhibit different release fractions when it appears in different cut sets within a major branch. Ideally, release fractions would be assigned by considering one cut set at a time. With millions of cut sets in a major branch, however, such a procedure is not feasible. If screening is used (and it appears essential for large fault trees), then release fractions must be assigned only once to each basic event, however many places it appears. This is an unavoidable limitation of the screening principle, at least as presently developed. Fortunately, post-screening detailed analysis of the relatively small number of surviving cut sets can include closer examination of release fractions for individual cut sets.

It is often possible to recast the fault tree so as to eliminate such release fraction problems. (This occurred in connection with the WFP rail transportation fault tree.) The resulting tree may be more complex than the original, but the increased accuracy may justify the change.

Another approach is to examine the release sequences in which the event with the conflicting release fraction requirements appears. The more pessimistic of the two possible values (or sets of distributed values) is then attached. In this way, no cut sets are mistakenly discarded because of the questionable release fraction. Later calculations can discard cut sets whose release fractions were purposely overestimated by this scheme.

One final difficulty is the fact that time behavior of release phenomena is not handled explicitly by the present procedures. The analyst should consistently treat all release fractions to arrive at some sort of

time-integrated or other meaningful treatment. Again, detailed hand calculations can treat time-dependent releases for surviving cut sets in whatever manner is appropriate.

7.6.4 Release Fraction Data

Generally, the same basic sources of release fraction data exist as for probability data: operating data, test data, analysis, and engineering judgment. However, most of the basic events with release fractions of interest relate to material transport under accident conditions. Operating data for such situations are generally quite sparse. More reliance must be placed on test and analysis documentation, which constitutes an extensive literature. Again, release fractions for many events can be assigned only by engineering judgment.

7.7 CHECKOUT OF THE COMPUTER CODES

A test fault tree (see Appendix H) was constructed to provide a check of the programming and operating validity of the FAULT, FAULTG, and RAFT codes against hand calculations. The test tree, consisting of about 500 cut sets, was purposely drawn so as to constitute a severe challenge within the constraint of a moderate number of cut sets.

Cut sets within the tree were identified by FAULT and compared against results from manual identification and from code ALLCUTS.⁽²²⁾ One branch of the tree, having a very high density of repeated cut sets and of cut sets with repeated basic events, was of particular interest in this part of the test.

The performance of the screening process of FAULT on the test tree was verified manually. The ALLCUTS code, which has similar screening provisions, was used as a backup check.

Cut set probabilities were hand-calculated for a tree branch containing various combinations of repairable and nonrepairable as well as online and standby components. Release quantities were also manually checked for this branch.

In all these tests, the FAULT and RAFT codes were found to agree with the results of manual calculations and of the ALLCUTS code. Slight differences in probability values were found between FAULT and ALLCUTS. The latter does not use the small probability approximation, discussed in Appendix C, 2.1. The approximation is always conservative. For basic event probabilities <0.1 , a condition usually satisfied, the resulting errors are small (about 5% for a one-event cut set).

Code FAULTG was used to analyze the same test tree. The results matched those obtained by use of FAULT.

THIS PAGE
WAS INTENTIONALLY
LEFT BLANK

8.0 THE TOTAL RISK OF THE POTENTIAL RELEASE SEQUENCES OF AN OPERATION

8.1 INTRODUCTION

The risk measure totals for the major branches of the fault tree, as calculated by RAFT, do not provide complete information regarding system risk. In addition to the fact that screening involves (approximate) calculation of only A and B terms, with $C \times D \times E$ to be calculated later and $A \times B$ values to be refined, two pieces of information are missing. This is illustrated in Figure 9.

FIGURE 9. Interrelationship of Groups of Potential Failure Sequences. The total risk of the operation is represented by the total area within the outside boundary of the diagram.

The first missing piece of information, represented by region 2 in the figure, involves the risk of the low-risk-measure cut sets discarded during screening. Code RAFT provides the risk-measure sum for only those sequences surviving the cutoffs. A large number of discarded cut sets, each with very low risk, could conceivably contribute a significant fraction of the total risk represented in the fault tree. Figure 3 shows that the risk-measure sum of the discarded cut sets is estimated then added to the RAFT-calculated sum for sequences of higher risk measure to give the total for the tree or major branch. Section 8.2 indicates how the risk-measure sum for the discarded cut sets is estimated.

Additional risk is represented by potential release sequences which do not appear on the fault tree. This risk is represented by region 3 in

Figure 9, whereas the risk of the sequences which were identified is represented by regions 1 and 2. Sequences may have been omitted because of simplification, oversight, lack of understanding of the system, or inability to conceive of all possible release sequences. There is no known method to furnish reliable predictions of even the approximate value of the risk sum of such omitted sequences. Other investigators (e.g., Reference 29) have addressed this difficulty, termed herein the completeness problem. However, they did not present detailed derivations and we have reservations about their methods (see Appendix J). Section 8.3 discusses this problem at greater length. Procedures are given for estimating the total risk of the operation, based on various observations and assumptions regarding the nature of the known and the unknown sequences, respectively.

8.2 THE RISK SUM OF THE DISCARDED SEQUENCES

The total risk measure of all sequences in a fault tree major branch which undergoes screening is

$$R^* = R_H^* + R_L^* \quad (4)$$

where R^* = total risk measure of all sequences in the major branch,

R_H^* = total risk measure of the sequences which survived screening,

and R_L^* = total risk measure of the discarded sequences.

The risk-measure sum of the surviving sequences,

$$R_H^* = \sum_{i=1}^{n_{\text{RAFT}}} A_i B_i, \quad (5)$$

is calculated by code RAFT. Here, n_{RAFT} is the number of unique cut sets which survive screening and are processed by RAFT. Typical values of n_{RAFT} are a few hundred to a few thousand. (If the C_i terms have been included, it is assumed either that they have been absorbed within the B_i terms or that they can be factored outside the summation.)

An estimate of the risk-measure sum of the discarded sequences,

$$R_L^* = \sum_{n_{RAFT}}^{n_T} A_i B_i, \quad (6)$$

is needed to determine if

$$R_L^* \ll R_H^* \quad (7)$$

i.e., whether the total risk measure for the discarded sequences is negligible compared to that for the surviving sequences. Here n_T is the total number of unique cut sets within the major branch. Typical values of n_T range from tens of thousands to millions.

It is not possible to precisely evaluate R_L^* if the screening process is used. This is because most cut sets are discarded on the basis on their low A_i values before being fed into RAFT for calculation of B_i . However, R_L^* can be either estimated or bounded from above. A conservative, approximate procedure was followed in an attempt to verify Equation (7), at least for the fault trees and values of n_{RAFT} and n_T encountered to date.

An upper bound, B_{max} , can be found for B_i , so that

$$R_L^* \leq B_{max} \sum_{n_{RAFT}}^{n_T} A_i. \quad (8)$$

Here B_{max} is taken to be the largest release quantity for any cut set in the major branch. A simple, conservative selection is

$$B_{max} = (TIA) (RF)_{max} \quad (9)$$

where $(RF)_{max}$ is the largest release fraction among the basic events. However, more detailed examination of the major branch generally reveals a smaller value for B_{max} . To obtain a meaningful bound, the smallest value which can be determined with reasonable effort should be used.

Next, a bound is required for the probability summation of Equation (8). Certainly, the fact that $A_i \leq A_{\text{cut}}$ for every i could be used. However, this bound is so crudely conservative as to make verification of Equation (7) impossible for some fault trees. It has been found more effective to use the equation

$$\sum_{n_{\text{RAFT}}}^{n_T} A_i = (n_T - n_{\text{RAFT}}) A_{\text{ave}}. \quad (10)$$

Here A_{ave} is the (arithmetic) average probability for all unique discarded cut sets.

In practice, calculating n_T and A_{ave} is difficult, again because of procedures to maximize screening efficiency. In FAULT and FAULTG, blocks of cut sets are discarded, by comparison with n_{cut} , before their probabilities are evaluated. The probabilities for these cut sets are unknown except that they are, by the derivation of n_{cut} (see Appendix D), less than or equal to A_{cut} . Furthermore, for efficiency, the blocks of cut sets discarded are not checked for duplicates. As the codes now stand, there is no way of knowing the number of duplicates in the discarded cut sets.

A conservative, approximate procedure has been added to the RAFT code to evaluate Equation (10). At the user's option, code FAULTG will put out to tape a list of cut sets discarded at the top gate. Cut sets not surviving the cutoffs at lower gates would exhibit even lower probability if carried along to the top gate. Therefore, those discarded at the top are expected to be of much higher probability than those discarded earlier. This provides a conservative sample for probability calculations.

Code RAFT accesses the above tape, which, for a major branch of a few million cut sets, may contain about 10,000 cut sets. Each entry on the tape includes the number of events in the cut set, their descriptors, and the cut set probability. RAFT removes duplicate cut sets, adds the probabilities of the remaining cut sets, and divides by their number. The result

is the arithmetic average of the probability of the unique cut sets discarded at the top gate. This is expected to be a very conservative estimate of the quantity, A_{ave} , for all unique discarded cut sets.

Since n_T is not known, the conservative value used is the total number of BICS in the major branch (including duplicates). This number is reduced by n_{RAFT} , then multiplied by A_{ave} and by B_{max} , to give an upper bound on R_L^* in Equation (8). Finally R_L^* is compared with R_H^* to determine whether the discarded sequences contribute significantly to the risk measure for the major branch.

In some fault trees, compounding of conservatisms in this way may lead to such unrealistically high upper bounds on R_L^* as not to satisfy Equation (7). This occurs despite the fact that the actual R_L^* value might indeed satisfy the equation. More precise bounding calculations for R_L^* would be considered. In limited application to date, however, no such difficulty has been encountered.

The very conservative procedure described above was applied to a large (1.6×10^6 BICS) major branch of the water basin storage fault tree.* The risk-measure sum of the discarded sequences was calculated to be <8% of the total in the major branch. This bounding estimate is probably high by orders of magnitude because of the conservative procedure for calculating A_{ave} . The risk-measure sum of the discards is probably <<1% of the total for the major branch.

8.3 THE RISK SUM OF THE OMITTED SEQUENCES

8.3.1 Definition of the Completeness Problem

Let us suppose that a nuclear operation has N (disjoint and/or low-probability) potential release sequences, designated 1, 2, ..., N . Each sequence i has a probability P_i of occurring in a given time period and a consequence c_i per occurrence. The "actual" risk R_a of the system may be taken to be the sum of the risks of all potential release sequences,

* In this case, the actual B_i values for cut sets discarded at the top level, rather than B_{max} , were used, resulting in a more accurate calculation.

$$R_a = \sum_{i=1}^N R_i \quad (11)$$

R_i , the risk associated with sequence i , is taken to be $P_i c_i$. If all N sequences are identified and the value of R_i is accurately determined for each sequence, R_a , the summation of the R_i values, will provide the actual risk of the system.

The term R_a may be better understood by a thought experiment. Imagine that the system is built and operates for a period very long compared to the expected interval between accidents contributing significantly to risk. From analysis of operating and accident data, the actual risk R_a of this system could be determined.

Few systems are of the type for which R_a is known. Indeed, for a system with sufficient operating experience, there would be no need for theoretical calculations of risk. One could merely examine the records of system operation and of accidents.

In practice, the objective of identifying and evaluating all of the N potential release sequences is seldom attainable. The human mind cannot enumerate all the potential failure sequences of a complex system. Sequences may also be omitted for simplification or because of oversight or lack of understanding of the system.

If one can identify and calculate the risk of only n ($< N$) of the sequences, then the calculated risk is

$$R_c = \sum_{i=1}^n R_i \quad (12)$$

and

$$R_c < R_a \quad (13)$$

The calculated risk R_c is a function of the time, t , spent in identifying potential sequences. As more effort and time are invested, more sequences will be identified. Eventually, however, the rate at which new sequences are found will approach zero.

If all major risk contributors and a majority of the minor contributors were identified and evaluated, R_c might approach R_a rather closely, as in Figure 10. However, if major sequences or large numbers of minor sequences were omitted, the time behavior of calculated risk might resemble that in Figure 11.

These two figures illustrate the completeness problem associated with risk analysis. The problem centers around those release sequences not identified and the relative importance of their contribution to the system's total risk. Questions which might be asked at the "completion" of a risk analysis include: What is the effect on R_c of the sequences not analyzed? Are any missing sequences critical; i.e., are their risks higher than those of the sequences which were found? Are there numerous small unidentified risks whose sum might represent a significant risk? How many missing sequences might be found per additional unit of analysis time? At what point, t_f , in analysis time can one assume that $R_c(t_f)$ is sufficiently close to R_a , given that the value of R_a is not known nor is the term "sufficiently close" well defined?

Such questions about completeness of a risk analysis of a complex system can never be fully answered. Even if the system operated for a very long time, only those failures which actually occurred could be logged. There would still be no absolutely reliable way to account for those yet to occur. It is hoped that the following discussion will, nonetheless, point the way to additional understanding of the completeness problem.

FIGURE 10. Calculated Risk as a Function of Time, with Most of the Risk Identified

FIGURE 11. Calculated Risk as a Function of Time, with Much of the Risk Not Identified

8.3.2 An Upper Bound on the Actual Risk of a System

The procedures described in this report (and in most of the references) lead to the predicted risk (or reliability) of a system. This result R_c was discussed in the preceding subsection. The risk of many systems of interest can be only predicted and not evaluated (i.e., demonstrated). This is because, although ample component data may exist, system operating data are insufficient to support an evaluation of system performance. The interactions among components may be too complex or not sufficiently well understood for the resulting prediction of system safety or reliability to be considered completely dependable.

As system data accumulate, the risk (or the reliability) can be evaluated, or at least bounded, by means of demonstration data.⁽³⁰⁾ This result, the demonstrated risk R_d , relates to the completeness problem. Under certain assumptions, the demonstrated risk can provide an upper bound for the actual risk R_a .

A simplified example illustrates the behavior of the demonstrated reliability r_d as system operating data accumulate. A system consisting only of a simple, one-shot, "go-no go" component is assumed. The demonstrated reliability of such a system can be calculated by means of a binomial distribution chart, such as that for 50% confidence level shown in Figure 12. (More complete charts appear in Reference 31.) Assume an "actual" reliability r_a of 0.99. Suppose 50 tests, or trials, are performed on these components, with no failures resulting. The lower confidence limit on r_d can be read from the upper abscissa of Figure 12. As the number of trials accumulates to 5 and on to 50, r_d follows the $F = 0$ (no failures) curve upward and increases from 0.87 to 0.986. If the 51st trial results in a component failure, we move to the $F = 1$ curve, and r_d drops to 0.966. Accumulation of 49 more successful trials results in $r_d = 0.983$. Thus, for one failure in 100 trials, r_d is within 0.007 of r_a . With 10 failures in 1000 trials, r_d is within 0.001 of r_a .

The value of r_d may fluctuate somewhat initially, but, as more data accumulate, it gradually approaches the "actual" reliability. Because r_d eventually approaches the value of r_a , the demonstrated reliability is

FIGURE 12. Upper Confidence Limit on Unreliability (one minus lower confidence limit on reliability). Confidence coefficient = 0.50.

helpful for bounding r_d . This approach must be used carefully, however. The quantity r_d is not always a conservative estimate. Suppose the failure occurred on the 100th trial (or even later). Then the lower bound on r_d would reach a peak value of 0.993 at 99 trials, before dropping to 0.983. In a word, this is why a statement of confidence level, e.g., 50%, is needed. (A chart corresponding to a 99% confidence level could have been used. The lower bound on r_d would have been only 0.935, given one failure in 100 trials.) At 50% confidence level, the number of trials must reach about 70% of the expected number of trials-before-failure (inverse of reliability) before a nonconservative value of r_d is possible. Therefore, this limitation on the conservatism of r_d is not severe. On the other hand, a rash of early failures would increase the conservatism of the r_d bound.

Another implicit assumption in this approach is independence of the trials. In reality, additional trials may increase the failure rate, as in the case of repeated testing of an aging component. More trials may also decrease the failure rate, as when a burn-in period is completed.

Reference 7 used the concept of demonstrated reliability, as follows: "Counting commercial and military power reactors, there have been almost 2000 reactor-years of experience with no nuclear accidents. This suggests that the likelihood of an accident is less than 10^{-3} per reactor-year." A calculation for 2000 trials and $F = 0$ substantiates the above conclusion at a confidence level of 86%. Thus, although insufficient system data were available to demonstrate the extremely low probability of severe reactor accidents, available data could nonetheless be used for an upper bound (at a given confidence level) on system failure probability.

Significant operating data are available for several other operations within the fuel cycle. An upper bound on system risk, at a given confidence level, can thereby be postulated for each such operation.

In conclusion, our experience tells us that the predicted system risk R_C , shown in Figures 10 and 11, cannot increase without bound. Such behavior would contradict the (limited) data from which the demonstrated risk is calculated.

8.3.3 Verification of Predicted Risk

Because of the extremely low probabilities of serious nuclear accidents, system data would have to be gathered over very long periods to validate the predicted risk. A more practical way to assess the accuracy of risk prediction methods might be to test them on systems with higher failure rates.

Green and Bourne⁽³²⁾ have compared predicted values of reliability with those actually achieved for about fifty systems or elements of systems. Values were calculated for the ratio ρ of the observed failure rate to the corresponding predicted failure rate. The median value of ρ was found to be about 0.82. About 60% of the ρ values were within a factor of 2 of unity.

94% were within a factor of 4. These figures are impressive. However, they were generally obtained from systems much less complex than major nuclear operations (an entire nuclear facility being thought of as a system).

8.3.4 Two Limiting Cases Related to Unidentified Risk

With the preceding material as background, it is now instructive to consider two limiting cases related to the nature of the unidentified release sequences. Real systems can be expected to fall between these two extremes. However, it is shown that formulating release sequences in a certain way can force the unidentified risk of some systems to approach that of the more tractable of the two limiting cases.

8.3.4.1 The Case of Generic Sequences

In this limiting case, the data permit the analyst to relate the identified sequences in generic groups. The collection of identified sequences then accommodates all possible release sequences. Further analysis might result in more sequences being identified, but the new sequences would be found to be merely special cases, subdivisions, or restatements of the more generic sequences. Figure 13 is a simple illustration of this case. The area within the outer boundary represents the actual risk of the system, R_a . The four numbered areas in the left diagram represent the respective risks of four rather generic identified sequences. The total area of the four sequences represents R_c , which, in the generic case, equals R_a . In the diagram on the right, further analysis has led to identification of sub-sequences 2a through 2e. However, aside from a possible increase in accuracy resulting from the subdivision, no risk area has been identified or added to R_c .

An actual nuclear operation approaching this limiting case is the rail shipment of solidified high-level waste. A PNL risk analysis of this operation involved formulation of the following four classes of accidents occurring during shipment: collision with other trains, derailment, other train-associated accidents (collisions with other types of vehicles, hot boxes, on-board fires and explosions, etc.) and accidents not associated with trains (falling aircraft, tornadoes, earthquakes, traveling through range fires, etc.). Data are available for the first three classes.

After a Given Period
of Analysis

After Additional Analysis

FIGURE 13. The Limiting Case in Which All Unidentified Sequences Are Contained Within the More Generic Sequences Which Have Been Identified

The analyst could generate innumerable specific accident sequences for these three broad classes. However, in general, no new risk would have been identified, because the specific sequences would be merely subdivisions of the generic accidents.

The fourth class of accidents is amenable to discovering additional external events which could lead to train accidents. Data obtained to date indicate that accidents in this class are extremely uncommon, however. Thus, for the rail shipment operation, unidentified sequences probably contribute very little to system risk. The accuracy of R_c is probably limited more by the accuracy with which the identified sequences have been evaluated. One example is the degree of uncertainty in the impact resistance of the shipping container.

Prediction of the risk which would be calculated for the maximum amount of sequence subdivision involves the same reasoning as that for handling potential absorption errors (Sections E.5 and E.6 in Appendix E). If the consequences of the more generic sequences are specified correctly,

considering all contingent events as in Appendix E, no amount of subdivision will alter the calculated risk. However, to specify consequences correctly requires knowledge of these contingent events. A "Which comes first, the chicken or the egg?" type of situation arises.

The accuracy of R_C , then, depends on the analyst's ability to specify, by explicit or implicit augmentation with contingent events, the consequences of the more generic sequences identified. The extent of subdivision required for R_C to approach R_a depends on the experience and insight of the analyst, the nature of the system, the form of available data, and the acceptable error. If available data properly include the effects of contingent events by being pre-compiled, subdivision of sequences may not be necessary. To some extent, data for the WFP rail transportation study are of this type. Other than this instance, we are unaware of studies of analysts' abilities to augment sequences properly. Such studies might indicate the relationship between R_C and R_a for systems approaching this limiting case.

8.3.4.2 The Case of Additional Risk

This limiting case is simply illustrated in Figure 14. Again the areas of the diagrams represent the actual risk R_a of the system. The four numbered areas in the left diagram represent the risks of four sequences identified after a given period of analysis. The shaded area represents the risk associated with unidentified sequences.

The diagram on the right shows that, after additional analysis, new sequences 5 and 6 have been identified. Although R_C has increased, it is still short of R_a by an amount represented by the area which remains shaded.

The calculated risk of real systems will tend to exhibit this type of behavior if the identified sequences are specific and nongeneric. In this sense, the event "commercial aircraft strikes building," for example, is considered rather specific. The event "airborne missile strikes building" is more generically described. It might include the impact of commercial aircraft, private and military aircraft, tornado-generated missiles, and other such hazards. Use of the first description leaves the way open

After a Given Period
of Analysis

After Additional Analysis

FIGURE 14. The Limiting Case in Which None of the Unidentified Sequences Is a Subdivision of the Identified Sequences

for unidentified sequences. Whenever data permit, use of the more comprehensive description along with its subcategories reduces the unidentified risk.

An analogy has been found helpful in thinking about this second limiting case. Imagine a large, sandy beach. A very large number of metal chunks of various sizes are hidden beneath the surface of the sand, not necessarily at random locations. Some chunks are quite large but many are very small. An analyst is given a metal detector and is allotted a specified length of time. He is to estimate the total amount of hidden metal, based on the amount he locates by walking about the beach during the search period. His probability of finding a given large chunk of metal is, of course, much higher than it is for a given small piece.

The crude analogy is easily transformed to the realm of risk analysis. Merely substitute system safety tools for metal detector, release sequence for metal chunk, analysis period for search period, magnitude of risk or of probability for size of metal chunk, and nuclear operation for sandy beach.

Of course, there is no rigorous way to know the total amount of metal (total risk) without actually finding all of the metal chunks (release sequences). However, various assumptions can be made about one's ability to find chunks (sequences) as a function of their size (risk or probability).

For a given assumption one can estimate the magnitude of the unidentified risk and, thereby, the actual risk R_a . Appendix K presents several ways in which this can be done. Estimates of unidentified risk are given for a liquid transfer system for high-level waste.

THIS PAGE
WAS INTENTIONALLY
LEFT BLANK

9.0 AN ALTERNATIVE SCREENING PROCEDURE BASED DIRECTLY ON RISK MEASURE

The screening procedure described in Sections 5.0 through 7.0 is based on the risk measure,

$$R^* = A \times B, \quad (2)$$

where A is the cut set probability and B the associated quantity of radioactive material released. A reference cut set is selected, against which other cut sets are compared. A probability cutoff is formulated by considering the risk measure of the reference cut set, the maximum conceivable release quantity, and an uncertainty factor. A cutoff on cut set length is derived from the cut set probability cutoff and the probabilities and unavailabilities for all basic events.

An alternative procedure has been formulated and applied. It involves screening based directly on risk measure. For certain applications it promises to displace the original procedure.

9.1 DERIVATION OF THE ALTERNATIVE SCREENING PROCEDURE

Expanding Equation (2) by means of equations in Section 7.6.2.3 gives

$$R^* = A \times (TIA) \times (RF_1 RF_2 \dots RF_n) \quad (14)$$

for a cut set of n events. For simplicity, it is assumed that any distributed release fractions are multiplied by their associated conditional probabilities before entry into Equation (14). The RF_i terms are thus the mathematically expected values of the release fractions.

Division by the total available inventory, which is assumed to be identical for all cut sets in the major branch, gives

$$\frac{R^*}{TIA} = A \times (RF_1 RF_2 \dots RF_n).$$

Appendix D derives this general equation for cut set probability:

$$A = z_1 Q_2 Q_3 \dots Q_n P_1 + z_2 Q_1 Q_3 Q_4 \dots Q_n P_2 + \dots + z_n Q_1 Q_2 \dots Q_{n-1} P_n. \quad (15)$$

P_i and Q_i are basic event probabilities and unavailabilities, respectively.

This equation holds for cut sets consisting of all repairable components (all $z_i = 1$), of all nonrepairable components (all $z_i = \frac{1}{n}$), or of m ($< n$) non-repairable components ($z_i = \frac{1}{m}$ or $\frac{1}{m+1}$, as appropriate). Inserting this result into the previous equation and regrouping terms gives

$$\frac{R^*}{TIA} = z_1(Q_2RF_2)(Q_3RF_3)\dots(Q_nRF_n)(P_1RF_1) + z_2(Q_1RF_1)(Q_3RF_3)(Q_4RF_4)\dots(Q_nRF_n)(P_2RF_2) + \dots + z_n(Q_1RF_1)(Q_2RF_2)\dots(Q_{n-1}RF_{n-1})(P_nRF_n). \quad (16)$$

If

$$P_i' \equiv P_iRF_i \quad (17)$$

and

$$Q_i' \equiv Q_iRF_i, \quad (18)$$

Equation (16) becomes identical to Equation (15), but with transformed variables:

$$\frac{R^*}{TIA} = z_1Q_2'Q_3'\dots Q_n'P_1' + z_2Q_1'Q_3'Q_4'\dots Q_n'P_2' + \dots + z_nQ_1'Q_2'\dots Q_{n-1}'P_n' \quad (19)$$

If the P and Q data are modified according to Equations (17) and (18), respectively, code FAULTG can be made to screen cut sets based on a modified risk measure (R^*/TIA) rather than on cut set probability. No programming changes to FAULTG are required.

Use of the n_{cut} cutoff may be retained. The cutoff value will change because the release quantities are incorporated. The A_{cut} cutoff (which actually becomes R_{cut}^* , a cutoff on risk measure) may also be used.

9.2 ADVANTAGES AND LIMITATIONS OF THE ALTERNATIVE PROCEDURE

The chief advantages of the alternative procedure are less computer running time and smaller storage requirements. Because each cut set is screened on its calculated release quantity, not on the largest release quantity in the major branch, fewer low-probability low-consequence cut sets are retained.

Otherwise, many low-probability cut sets (millions, in some cases) would have to be analyzed to assure that a few with high release quantities would not be lost in the screening.

The new method also facilitates a better estimate of the risk-measure sum of the discarded cut sets. This is because of more accurate treatment of the B terms.

Another advantage is increased flexibility in use of a risk measure cut-off. Such might be used to retain all cut sets above a certain minimum value of risk measure. Although RAFT does incorporate such a cutoff, the new procedure again reduces the number of cut sets carried along from FAULTG.

A final advantage is elimination of the need to use two computer codes (FAULTG and RAFT).

The limitations of the alternative procedure relate to loss of information. This results from the combination of probability data with release fraction data before entering FAULTG. For example, no cut set probabilities can be furnished the user without manual calculations. The same holds for values of the release quantity. No information is furnished regarding the sub-cut sets. Finally, a technique under evaluation for handling severe environment common-cause effects is not compatible with use of the alternative procedure.

In summary, the alternative procedure is favored if computer running time or storage capacity is of concern, or if the user is interested only in values of the risk measure. For analysis of manageable major branches, for knowledge of cut set probability and consequences, or for common-cause studies, the original procedure is preferred.

**THIS PAGE
WAS INTENTIONALLY
LEFT BLANK**

10.0 PRELIMINARY EVALUATION AND SCREENING WITH NO ASSUMED FORM OF THE RISK EXPRESSION

The procedures for preliminary evaluation and screening can accomodate any simple risk expression in place of the form (probability times consequences) presently used. Use of a specific risk expression can also be completely bypassed so as to screen essentially on probability rather than on risk. The results of this more general analysis can be displayed simply as probability versus consequences, as in Reference 7. This section describes how these optional procedures are accomplished.

10.1 BACKGROUND REGARDING PROBABILITY, CONSEQUENCES, RISK, AND VALUE

The procedures described thus far in this report treat risk as being linearly proportional to probability P and to consequences c :

$$R = P \times c. \quad (20)$$

More precisely, the sum of the individual risks R_i from n potential accidental release sequences is expressed as

$$R = \sum_{i=1}^n R_i = \sum_{i=1}^n P_i \times c_i. \quad (21)$$

This dual linearity assumption is used in deriving the value of the probability cutoff A_{cut} . See Equation (3), in Section 7.4.2. It is also used to rank the sequences, within similar groups, based on the risk measure $A \times B$. See Equations (1) and (2), in Sections 6.2 and 6.3.1, respectively.

The dual linear expression defines the risk of an accident as the probability that the accident will occur, multiplied by the consequences (losses, insults) which ensue. The risk is thus the expected consequences, or the expected loss. Many safety studies of nuclear operations

(e.g., References 7,* 13, 16) have defined risk in the form of Equation (20) or by integration of a different form of Equation (20).

However, risk can be expressed in forms other than that of Equation (20). For example, Farmer⁽¹⁷⁾ used a risk limit line with a $c^{3/2}$ dependence. Analogously, in business decision theory, the criterion for selection among alternatives is not always the most favorable expectation, that is, the best average gain or least average loss. The "maximin" criterion of maximizing the minimum expected gain⁽³³⁾ is sometimes used. Two additional criteria involve "optimism" and "pessimism."⁽³³⁾ In the former, the alternative with the greatest possible gain is selected, without regard to probability. In the latter, the alternative with the smallest possible loss is the choice, again independent of probability. The pessimism principle might be used if a loss of given magnitude would bankrupt a firm.

The present procedures can accept any simple definition of risk. For example, Equation (20) might be generalized to $R = P^m \times c^n$, with values of m and n specified.

However, studies by Rowe⁽³⁴⁾ show that the notion of risk is generally too complex to be modeled merely by changing the functional relationship of Equation (20). It is not simply the magnitude of the consequences that is meaningful to risk-takers, but their value (a subjective criterion). While the magnitude of the consequences can generally be estimated, the value of the consequences is elusive. Different valuing agents (people or groups of people) may assign different values to the same consequence. The valuation function of even the same individual will most likely change with time. These arguments show the desirability of safety analysis methods free of any assumed form of the risk equation.

As an option, the preliminary analysis and screening procedures can be accomplished so as to satisfy the above requirement. The analysis results

* Reference 7 did not explicitly apply the defined risk expression in performing the analysis or in presenting the results. Accident probabilities and consequences were simply plotted against each other in the form of complementary integral density functions.

would appear in the same format as in Reference 7. The following section discusses the modified procedures which avoid dependence on expressions of the form of Equation (20).

Unfortunately, results obtained from these optional procedures, or from any risk analysis not assuming a specific risk expression, have certain limitations. For example, consider potential accidents 1 and 2, the former having the higher probability but also the smaller consequences. In the absence of a specified risk function, risk comparisons are not possible between accidents 1 and 2. Such comparisons are possible only if the two accidents have equal probabilities or equal consequences or if the probabilities and consequences of one accident are both larger than those for the other accident. Another limitation concerns the concept of negligibility in comparing the risks of two potential accidents. Without a risk function, one can state that some accidents are of greater risk than others, but not how much greater. Thus the generality which results from eliminating risk functions also diminishes one's ability to compare the importance of potential accidents.

10.2 MODIFICATIONS REQUIRED FOR THE OPTIONAL PROCEDURES

10.2.1 Determining the Values of A_{cut} and n_{cut}

The value of the probability cutoff A_{cut} was derived earlier by comparing preliminary values of sequence risk measures against that for a reference sequence. Equation (3), derived from Equation (20), facilitated comparisons between accidents having different probabilities and different consequences. The chain length cutoff n_{cut} was then derived from A_{cut} and from the data for the basic events. In this sense, the cutoff values were derived, not arbitrary.

For the optional procedures, the cutoff values can be developed without the use of expressions such as Equation (3). The approach is changed only slightly, and much of the earlier discussion is appropriate. It is noted in passing that the cutoff values are of no philosophical significance

by themselves. They are merely tools used to terminate computer searches at a specific level of behavior. The cutoffs can be adjusted up or down as desired.

Most simply, the value of A_{cut} can be arbitrarily established at some very low value. The consequence plots in Reference 7 terminated at a probability of 10^{-9} /reactor-year, although individual sequences were listed with probabilities as low as 10^{-12} . Because the dominant sequences, for a given magnitude of consequence, typically had probabilities of 10^{-6} to 10^{-4} , a probability cutoff placed at 10^{-12} probably would not have resulted in discarding any significant individual contributors. A value of 10^{-12} is also close to the cutoff values of 10^{-10} to 10^{-11} used in the Waste Fixation Program risk analysis.

The value of A_{cut} can also be determined in a more rigorous fashion. One considers those release sequences in the major branch under study which have the highest potential release quantity, B_{max} . (Differences in C terms will have been taken into account.) From among these sequences of greatest potential release, one identifies a sequence whose probability is near the highest in that class. (If the sequence selected does not have the highest probability in the class, the screening will simply be slightly less efficient.) This sequence is called the new reference sequence; its probability is denoted $A_{\text{max}}|B_{\text{max}}$.

All other sequences have a consequence no greater than that of the reference sequence. Therefore, any sequence whose probability is much smaller than $A_{\text{max}}|B_{\text{max}}$ is considered much less important than the reference sequence. Mathematically, for a given sequence with

$$A \leq M A_{\text{max}}|B_{\text{max}}, \quad (22)$$

where $M \ll 1$,

$$R^*(A,B) \ll R^*(A_{\text{max}}|B_{\text{max}}, B_{\text{max}}) = R^*(\text{reference sequence}). \quad (23)$$

This is true, regardless of the value of B for the sequence, because $B \leq B_{\max}$ by definition. Note that no form of the risk measure function R^* has been assumed. It is only assumed that the importance of a sequence increases with its probability and its consequences.

As discussed earlier, the factor M allows for uncertainties in calculations of A and of $A_{\max} | B_{\max}$. Values of 10^{-2} to 10^{-4} for M appear reasonable.

If an equality is used in Equation (22), the quantity A so defined is termed the probability cutoff A_{cut} . All sequences with values of $A \leq A_{\text{cut}}$ are of much less importance than the reference sequence.

Use of the second method for determining A_{cut} ensures that no important sequences of extremely low probability and high consequences will be discarded. The first method can also accomplish this if the arbitrary cutoff for probability is wisely selected.

No matter how A_{cut} is determined, the original technique is unchanged for calculating n_{cut} . It uses the values of A_{cut} and of the probability descriptors (P_i , Q_i , m_i) for all basic events in the major branch. Here m_i indicates whether the component is repairable. See Appendix C, 3.1.

Thus, the cutoffs can be determined without recourse to any assumed form of the risk equation and without concern about losing low-probability, high-consequence sequences.

10.2.2 Presenting the Screening Results

The screening results can be presented as a histogram of sequence probabilities and consequences (see Figure 15), also without any assumptions about the risk expression. The general approach of Reference 7 would be followed. There, the almost continuous distribution of release quantities was simplified by assigning each sequence to one of nine (for PWRs) ranges of release, or release categories. The categories differed from one another in radionuclide mix as well as in release quantity. The probabilities of the sequences within each category were added, giving the total probability for each release category.

FIGURE 15. The Analysis Results Could be Presented as a Histogram of Radionuclide Releases

It is noted that simply listing a few dominant sequences in each category and summing these probabilities within a category does not necessarily constitute a complete presentation of results. The sum of the probabilities of a very large number of nondominant sequences in a category might well be significant compared with the sum for dominant sequences only. Techniques for treating this problem within the earlier screening procedure were discussed in Section 8.2. As described in Appendix G, the "branch residual sum" feature of RAFT provides a sum for the nondominant accidents which were identified.

11.0 DETAILED ANALYSIS PHASE

11.1 OVERVIEW

The computerized screening facilitates determination of which cut sets are the dominant risk contributors and merit further analysis. Such a tool is necessary because 1) detailed analysis of every cut set is not practicable; and 2) there is no simple way to determine which cut sets are important, short of some preliminary numerical analysis of the type described.

For the reasons listed below, the output from the screening generally does not constitute a suitable final answer for system risk even when the risk estimates for discarded sequences and omitted sequences (Figure 9) are included. Individual analysis of dominant sequences should follow. (Other systems safety techniques, such as event trees and cause/consequence diagrams, have limitations regarding final answers similar to those of the fault tree screening.⁽⁹⁾ However, the two methods mentioned do offer at least conceptual advantages in handling the time-sequencing of events in detailed analyses. On the other hand, Burdick et al.⁽³⁵⁾ have recently applied phased mission techniques to fault trees for nuclear systems. The techniques are currently limited to nonrepairable components.)

- The A and B values developed were approximate. Additional analyses and testing may be needed for improved values.
- Spectrum (distribution) aspects of certain A, B and C terms may need detailed treatment. For example, a range of possible temperatures in a facility fire may be considered in assessing containment failure probabilities, plateout fractions, and radionuclide volatilities. Other investigators have performed analyses of this type for earthquakes, for fuel bundle drops, and for loss-of-coolant accidents. Accuracy is generally improved if distribution curves, rather than point estimates, are used to analyze such situations.

- Detailed C x D x E calculations are necessary. (In some cases, C term considerations will have been included in the B term.)
- The screening generally requires use of the same release fraction for an event regardless of the sequence in which it appears (Section 7.6.3). In a detailed analysis, the context of each sequence would be studied before release fractions were assigned.
- Certain aspects of the time sequencing of events within a cut set can be handled on the fault tree (e.g., Reference 35). However, only through individual examination can the implications of event order within cut sets be adequately treated. The equations of Appendix C were developed under broad assumptions; for specific cut sets the sequencing of events can require adjustments to the equations. For example, it may be discovered that event 3 must always precede event 4 in the cut set, whereas the equations in Appendix C include all permutations of events unless standby and online components are involved. Furthermore, the consequences of a sequence may depend on the order of its events. Subtleties in repair and maintenance procedures can have similar effects. Fussell⁽³⁶⁾ has discussed the treatment of repair times for secondary failures.
- There is another limitation in the present treatment of severe environments. Although the common-cause nature of the occurrence of the environment is suitably modeled, dependencies exist among inhibit gates representing the structural responses of various components. These dependencies are not suitably modeled at present. A technique for improved treatment of these dependencies is under development.
- The fault trees constructed for screening and preliminary analysis include a rather generic treatment of certain types of common cause failure (CCF). Examples are utility outages and severe environments.

Although CCF analysis is a key part of system safety studies, complete CCF analysis of a large fault tree is not practicable. Thus, most CCFs are not identified in the preliminary analysis.

Although the above qualifications apply to the output of screening and preliminary evaluation, the present method still has utility for detailed evaluations. The various calculations (mostly manual) suggested above can be performed and factored back into the code system, thereby minimizing manual calculation time.

Several of the above limitations are discussed at greater length in this section. Although PNL methodology in most of these areas is not completely developed, progress to date is discussed. Included are spectrum considerations, identification of common cause failures and mathematical treatment of identified dependent events, and sensitivity and importance studies. As progress is made in these areas, reports documenting the results are planned.

11.2 SPECTRUM CONSIDERATIONS

As discussed in Section 4.6, many events appearing on nuclear safety fault trees are not simple on-off situations. A wide spectrum of outcomes is possible. One example is the effect of an earthquake on a facility. If an earthquake were to occur at a site, one of low severity is the most probable. However, given that it occurs, it also has the lowest conditional probability of inflicting damage. An earthquake of high severity is just the opposite. Only detailed examination of the curves of frequency versus severity and of conditional probability of damage versus severity can determine which severity contributes most to system failure.

Reference 4 reviews techniques for handling the spectrum problem, derives additional equations, and illustrates application to fault trees. PNL analysis experience in this area has included HEPA (high-efficiency particulate air) filter failure by tornadoes and impact failure of rail shipping casks for high-level waste.

11.3 DEPENDENT EVENTS/COMMON CAUSE FAILURES

11.3.1 Background

Consideration of commonality among faults, variously called the study of dependent events or of commoncause failures* (CCF), is vital to systems safety. The commonality may involve a failure in one system causing a failure in another system or an adverse environment causing simultaneous failures in more than one system. Overlooked CCFs can lead to errors of orders of magnitude in calculated probability, often overshadowing uncertainties in component failure data.

Simple redundancy does not remedy CCF problems. CCF could negate the efficacy of redundant safety systems. CCF data compiled by Epler at Oak Ridge and in Canada and Britain indicate that redundancy of greater than a factor of two contributes very little to system reliability.^(37,38) Simply increasing the test frequency is also of little avail because, as in most occurrences reviewed by Epler, the failure propagation is almost instantaneous. Such defenses as functional diversity, physical separation, inspection, testing, safe failure modes, and administrative controls all must be considered.

Two aspects of CCF analysis are treated here. The first, discussed in the rest of 11.3, concerns identification of CCFs. The second, presented in Appendix I because of its complexity, involves mathematical treatment of CCFs so identified. Probability expressions are derived for two types of dependency: mutually dependent loading and common external generalized stress. For both types, dependent events connected by AND or OR gates are treated. Review of Appendix IV of Reference 7 is recommended prior to reading Appendix I.

The generality of the probability equations of Appendix I for common-gate dependency is shown by the following argument. In theory at least,

* The term "common mode failures" is less accurate than "common cause failures." The components in question often do not fail in the same mode, but, if dependencies are present, they do fail from the same cause, either directly or indirectly.

any fault tree can be recast into a common form in which all the basic events of each cut set are inputs to a common AND gate. All cut sets are then inputs to a common OR gate immediately below the top event of the tree. An example appears in Figure 16. This rearrangement allows dependency between events X_1 and X_3 , not inputs to a common gate in the original tree, to be handled by equations for dependencies in a common gate.

A. ORIGINAL FAULT TREE

$$\begin{aligned} \text{TOP} &= (X_1 \cup X_2) \cap [X_3 \cap (X_4 \cup X_5)] \\ &= (X_1 \cap X_3 \cap X_4) \cup (X_1 \cap X_3 \cap X_5) \cup (X_2 \cap X_3 \cap X_4) \cup (X_2 \cap X_3 \cap X_5) \end{aligned}$$

B. RECAST TREE

$$\text{TOP} = \text{SAME AS IN ORIGINAL FAULT TREE}$$

FIGURE 16. Recasting Fault Trees into a Common Form.

11.3.2 Review of Existing Common Cause Failure Methods

Several current techniques (Reference 7, Appendix IV; References 39 and 40) for treating CCF were reviewed. The three efforts all relate to reactor protection systems. The General Electric CCF effort⁽³⁹⁾ amounted to 3 man-years. It is estimated that the investment of Reference 7 was comparable. The report of the GE work stated that because a complete CCF study would have been a gargantuan task the scope was bounded. The work involved considerable computer usage. The Reference 7 work apparently involved no computer usage directly related to CCF analysis. Only comparisons against the effects of data uncertainties were automated. Surprisingly, only Reference 39 stated that the CCFs were significant.

11.3.3 A Recommended Approach for Common Cause Failure Analysis

PNL has directed little explicit effort to date toward developing CCF analysis methods. This section presents some observations on potential CCF oversights and a recommended approach for CCF analysis. The approach combines existing CCF methods with new concepts.

11.3.3.1 Points in the Risk Analysis at Which CCF Errors Could Arise

Current PNL procedures for drawing fault trees already account for several types of CCF in a preliminary way. This results from the practices of 1) drawing one very large fault tree (rather than several smaller separate trees) for a given facility and allowing events to appear repeatedly at several locations on the tree; 2) including potential secondary failures from severe environments (both site-induced and facility-induced) for essentially every component of interest in the facility; and 3) including utility (power, water, air, etc.) outages for every component involved. However, there are three points in the analysis at which CCFs could be overlooked:

1. The fault tree must be correctly drawn, in that all significant component interactions contributing to the top event are properly displayed. At this point, one need not know whether the component interactions are independent or dependent; that will be determined later. If the interaction does not appear on the tree, one will not

have the opportunity to ascertain whether the events are independent or dependent. If the tree is correctly drawn, no cut sets representing potential CCFs will be lost at this point in the analysis. All CCFs will be included in the collection of cut sets. The only pitfalls would lie in the following steps, in which dependencies within a cut set might be missed.

2. With any screening process (including those based on cut set length), a cut set whose probability is below the cutoff value when its unique events are considered independent could exceed the cutoff if dependencies between events were included. The only known defense against this pitfall is the bounding combinations approach discussed in Reference 7, Appendix IV. A bounding check on CCFs could probably be added easily to FAULTG. However, using this approach would reduce the efficiency of screening.
3. In the postscreening review of cut set probabilities, dependencies among events in a cut set could be missed. An n-term cut set could even "collapse" to an m-term ($m < n$) cut set, typically increasing cut set probabilities by orders of magnitude. Painstaking examination of every significant and potentially significant cut set is needed. Hopefully, concepts described below will lead to identifying large numbers of potential CCFs by computer techniques, followed by individual examination to evaluate the more subtle dependencies. Only in this way can large numbers of cut sets be examined without inordinate expense.

There are other CCF phenomena not examined here. One such class of dependency is that between release events and pathways to man (e.g., a tornado resulting in release of radioactive material also alters local meteorology). These classes of dependency are generally less important than the pitfalls described above.

11.3.3.2 Overview of a Proposed Defense Against the Principal CCF Hazards

Defense against the three principal CCF pitfalls should be established. Critical review of fault trees by independent in-house safety

personnel, by operating personnel, and by consultants is a relatively sound defense against pitfall 1. The conservative bounding approach of Reference 7 is promising against pitfall 2, but it may seriously reduce screening efficiency. The following section outlines a procedure for use against pitfall 3, part of the procedure being computerized for efficiency. The approach is similar to that of Wilson et al.⁽⁴¹⁾

11.3.3.3 Outline of a Proposed Procedure for Defending Against the Third CCF Pitfall

It is assumed that the cut sets have been identified and correctly screened, leaving only those of actual or potential significance.

A list is prepared of potential causes of CCF. Table 1, comprising 12 categories is an example list. (The word "common" in Table 1 means "shared together" rather than "prevalent.")

Each basic event in the fault tree is then assessed for its potential susceptibility to each CCF cause of Table 1. Table 2 may be of assistance.

A computer code then uses the results of these analyses to search all significant cut sets for common susceptibilities among two or more basic events in the same cut set. Such cut sets are flagged for retrieval. Analysts systematically examine these cut sets to ascertain whether CCF could indeed occur. Comparing these with CCF preventive measures listed in Table 3 may be helpful, as may Jacobs'⁽³⁹⁾ procedure, described in Table 4.

Mathematical procedures for estimating probability bounds related to CCFs are discussed in Reference 7, Appendix IV: Equations 20-22 help in formulating an upper bound. Lower bounds are often calculated simply by assuming independent failures. More precise calculations are facilitated by Equation 28 of that volume or by the more detailed treatment of Appendix I herein.

Quantitative analysis of CCF phenomena^(42,43) will likely prove elusive. Probably only bounding values and rough estimates of dependency will be possible. However, a systematic procedure like that outlined here is considered valuable for identifying the most significant CCFs.

TABLE 1. Potential Sources of Common (or Shared) Cause Failure

1. Common Functional Deficiency

Misunderstanding of process variable behavior and relevance	Inappropriate instrumentation
Inadequate design protective action	Change in system characteristics
2. Common Design Error

Unrecognized interdependencies between subsystems, components	Dependence on the performance of equipment whose failure initiated the need for protection
Unrecognized dependence on common element	
3. Common Manufacturing or Installation Error

Manufactured in the same lot or by the same process	Incorrect installation by the same person or under the same procedure
---	---
4. Common Test, Maintenance, or Repair Error

Miscalibration	
Inadequate testing - inaccurate determination of component's condition	
Testing-initiated fault - the testing itself leaves the component in a fault mode	
Maintenance- or repair-initiated fault - the maintenance or repair itself leaves the component in a fault mode	
5. Other Common Human-Initiated Error

Operational errors	Procedural errors
Communication errors	
6. Common Normal External Environment

Dust	Humidity
Corrosion, oxidation, and other chemical reactions	Vibration
Temperature and thermal stresses	Radiation
7. Common Facility-Related External Phenomena

Fire	
Explosion	
Other energy sources within the facility (kinetic energy, gravitational potential energy, steam lines, etc.)	
8. Common Site-Related External Phenomena

Tornado, hurricane, lightning	Earthquake, geologic faulting
Flood	Plane crash, meteorite
9. Common Secondary Failure from Abnormal Condition in Transport Lines (blockage, short circuit, surges, etc.)

Steam	Water
Air	Mechanical drive shaft
Electricity	
10. Common Failure Due to an Initiating Failure

Failure of one pump results in greater load on second pump, accelerating its failure	
--	--
11. Failure Due to Common Dependence on Utility

Steam	Electricity
Air	Water
12. Common Physical Location (with an initiating event from one of the other categories)

TABLE 2. Properties Indicating Potential Common Cause Susceptibility.⁽⁷⁾
(Numbers refer to entries in Table 1.)

1. All components identical in type and specification (1, 2, 3)
2. Components all under the same maintenance and test (4)
3. All components having similar failure sensitivity (6, 7, 8, 9)
4. Components all in the same location (5, 6, 7, 8, 9, 10, 11)
5. Components all exposed to a possible accident environment (7, 8)
6. All components loaded or degraded by a previous failure (9, 10, 11)
7. All component failures human-initiated (5)

TABLE 3. Common Cause Failure Preventive Measures^(39,40)

Failure Category	Possible Preventive Measures
External Normal Environment	Functional Diversity - The use of different plant parameters involving different instrumentation in different locations to provide protection against a given event Design Administrative Control Safe Failure Modes Proven Design Standardization Equipment Diversity
Design Deficiency	Functional Diversity Physical Separation Design Administrative Controls - design reviews, qualification testing Operational Administrative Controls Safe Failure Modes Equipment Diversity
Maintenance Errors	Functional Diversity Operational Administrative Controls - requiring different persons to do certain tasks or requiring a second person to check on the first Equipment Diversity
External Phenomena	Functional Diversity Physical Separation Design Administrative Controls Safe Failure Modes Equipment Diversity
Functional Deficiency	Functional Diversity Design Administrative Controls Operational Administrative Controls Equipment Diversity

TABLE 4. Jacobs' Procedure for CCF Analysis⁽³⁹⁾

1. Assume an initiating event.
2. Track the resulting action until the system is safely in a stable condition in one of its normal modes of operation or shutdown.
3. Identify the plant parameter (level, pressure, flux, etc.) whose out-of-limits condition initiated the safety action.
4. Common mode fail all information on that particular parameter.
5. Assume the same initiating event and retrack the resulting action taking no credit for the failed parameter.
6. Repeat for enough carefully selected combinations of initial conditions to assure that the worst case is covered.
7. Restore the first common mode failure and fail another, repeating the whole analysis. Continue until all parameters that can contribute to success have been independently failed.
8. If a CMF case is found which is not backed up by functional diversity, then it may be necessary to analyze and employ one of the other diversities as an antidote.

11.4 SENSITIVITY AND IMPORTANCE STUDIES

PNL has not developed new methods for sensitivity and importance studies of fault trees. Existing concepts (e.g., References 5, 7, 44, 45) are promising. No particular difficulty is foreseen in adapting some of these concepts to PNL procedures. Because of the screening procedure, consideration must be given to sensitivity effects on discarded sequences as well as on retained sequences.

THIS PAGE
WAS INTENTIONALLY
LEFT BLANK

12.0 REFERENCES

1. T. H. Smith et al., "A Methodology for Risk Analysis of Nuclear Waste Management Systems," presented to the American Nuclear Society 20th Annual Meeting, BNWL-SA-4899, Battelle, Pacific Northwest Laboratories, Richland, WA, June 1974.
2. D. L. Streng, E. C. Watson and J. K. Soldat, Review of Calculational Models and Computer Codes for Environmental Dose Assessment of Radioactive Releases, BNWL-B-454, Battelle, Pacific Northwest Laboratories, Richland, WA, in publication.
3. H. C. Burkholder et al., "Migration of Radionuclide Chains Through an Adsorbing Medium," BNWL-SA-5079, Battelle, Pacific Northwest Laboratories, Richland, WA, December 1974.
4. T. H. Smith, Probabilistic Risk Analysis of Nuclear Systems, BNWL-1848, Battelle, Pacific Northwest Laboratories, Richland, WA, September 1974.
5. D. F. Haas, "Fault Tree Analysis," course notes, Joint Center for Graduate Study, Richland, WA, February 1974, to be published in book form.
6. H. E. Lambert, Systems Safety Analysis and Fault Tree Analysis, UCID-16238, Lawrence Livermore Laboratory, University of CA, May 1973.
7. USAEC, Reactor Safety Study, An Assessment of Accident Risks in Commercial Nuclear Power Plants, WASH-1400, draft, August 1974.
8. McDonnell Douglas Astronautics Company, Site Defense System Safety Program Plan, MDC G4550, May 1973.
9. D. S. Nielsen, "The Cause/Consequence Diagram Method as a Basis for Quantitative Reliability Analysis," presented at the ENEA/CREST Meeting on Applicability of Quantitative Reliability Analysis of Complex Systems and Nuclear Plants in its Relation to Safety, Munich, May 1971.
10. D. S. Nielsen et al., "A Cause-Consequence Chart of a Redundant Protection System," IEEE Transactions on Reliability, R-24, pp. 8-13, April 1975.
11. P. Rubel, "BONSAI: Cultivating the Logic Tree for Reactor Safety," Proceedings of the 1975 Annual Reliability and Maintenance Symposium, pp. 13-17, Washington, D.C., January 1975.
12. G. R. Burdick and J. B. Fussell, "On the Adaptation of Cause Consequence Analysis to U.S. Nuclear Power Systems Reliability and Risk Assessment," in A Collection of Methods for Reliability and Safety Engineering, Aerojet Nuclear Company, ANC 1273, Idaho Falls, ID, June 1975.

13. T. I. McSweeney et al., Transportation Safety Studies: The Risk of Plutonium Shipments, BNWL-B-295, Battelle, Pacific Northwest Laboratories, Richland, WA, 1973.
14. B. J. Garrick, "Accident Analysis," Holmes and Narver, Inc., Communication to Saul Levine, USAEC, November 18, 1974.
15. R. R. Fullwood and R. C. Erdmann, "On the Use of Leak Path Analysis in Fault Tree Construction for Fast Reactor Safety," Proceedings of the Fast Reactor Safety Meeting, USAEC, CONF-740401-P3, pp. 1493-1507, April 1974.
16. R. Cooperstein et al., Hazards Analysis of a Generic Fuel Reprocessing Facility, Final Report, SAI Services, May 1974.
17. F. R. Farmer, "Reactor Safety and Siting: A Proposed Risk Criterion," Nuclear Safety, vol. 8, pp. 539-548, 1967.
18. T. H. Smith and W. A. Ross, Impact Testing of Vitreous Simulated High-Level Waste in Canisters, BNWL-1903, Battelle, Pacific Northwest Laboratories, Richland, WA, May 1975.
19. R. K. Weatherwax, Jr., "Probabilistic Risk Analysis: Its Virtues and Limitations," presented to the American Physical Society, Washington, D.C., April 1975.
20. P. A. Crosetti, Computer Program for Fault Tree Analysis, DUN-5508, Douglas United Nuclear, Inc., Richland, WA, April 1969.
21. P. A. Crosetti, Fault Tree Simulation Computer Program, DUN-7697, Douglas United Nuclear, Inc., Richland, WA, June 1971.
22. W. J. Van Slyke and D. E. Griffing, ALLCUTS, A Fast Comprehensive Fault Tree Analysis Code, ARH-ST-112, Atlantic Richfield Hanford Company, July 1975.
23. P. K. Pande, M. E. Spector and P. Chatterjee, Computerized Fault Tree Analysis: TREEL and MICSUP, Publication ORC75-3, Operations Research Center, University of California, Berkeley, CA, April 1975.
24. J. B. Fussell et al., MOCUS-A Computer Program to Obtain Minimal Sets from Fault Trees, ANCR-1156, Aerojet Nuclear Company, Idaho Falls, ID, August 1974.
25. P. Chatterjee, Fault Tree Analysis: Min Cut Set Algorithms, AD 774 100, University of California, Berkeley, CA, January 1974.
26. P. W. Marriott et al., "The Loss-of-Coolant Accident and the Environment--A Probabilistic View," presented to the Winter Annual Meeting of the American Society of Mechanical Engineers, New York, NY, 72-WA/NE-9, November 1972.

27. I. M. Jacobs, "Assessment of Risk in Reactor Safety," presented to National Topical Meeting on Water Reactor Safety, CONF-730704, Salt Lake City, UT, March 1973.
28. General Atomic Company, GCR Accident Initiation and Progression Analysis, Progress Report for the Period February 1 Through June 30, 1974, GA-A13094, October 1974.
29. H. J. Otway and R. C. Erdmann, "Reactor Siting and Design from a Risk Viewpoint," Nuclear Engineering and Design, vol. 13, pp. 365-376, 1970.
30. U.S. Department of Defense, Reliability Evaluation from Demonstration Data, Military Standard MIL-STD-757, June 1964.
31. D. L. Lloyd and M. Lipow, Reliability: Management, Methods and Mathematics, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1962.
32. A. E. Green and A. J. Bourne, Reliability Technology, Wiley-Interscience, London, 1972.
33. J. E. Freund and F. J. Williams, Elementary Business Statistics: The Modern Approach, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1964.
34. W. D. Rowe, An Anatomy of Risk, Draft, Environmental Protection Agency, Washington, D.C., March 1975.
35. G. R. Burdick et al., "The Implementation of Phased Mission Techniques to Nuclear Systems Analysis," in A Collection of Methods for Reliability and Safety Engineering, Aerojet Nuclear Company, ANC 1273, Idaho Falls, Idaho, June 1975.
36. J. B. Fussell, "On the Analysis of Causes of Component Malfunctions During System Reliability and Safety Assessment," in A Collection of Methods for Reliability and Safety Engineering, Aerojet Nuclear Company, ANC 1273, Idaho Falls, ID, June 1975.
37. E. P. Epler, "Common Mode Failure Considerations in the Design of Systems for Protection and Control," Nuclear Safety, vol. 10, pp. 38-45, January-February 1969.
38. E. P. Epler, "The ORR Emergency Cooling Failure," Nuclear Safety, vol. 11, No. 4, pp. 323-327, July-August 1970.
39. I. M. Jacobs, "The Common Mode Failure Study Discipline," IEEE Transactions on Nuclear Science, 1970.
40. W. C. Gangloff and T. H. Franke, "An Engineering Approach to Common Mode Failure Analysis," presented at the Symposium on the Development and Application of Reliability Techniques to Nuclear Plants, Liverpool, Great Britain, April 1974.

41. J. R. Wilson et al., "Techniques for Qualitative Analysis of Common Cause Failures," in A Collection of Methods for Reliability and Safety Engineering, Aerojet Nuclear Company, ANC 1273, Idaho Falls, ID, June 1975.
42. W. J. Houghton et al., "Methods of Probabilistic Safety Analysis for Gas-Cooled Reactors," Transactions of the American Nuclear Society, vol. 21, pp. 210-211, 1975.
43. F. L. Leverenz et al., "A Dependent-Event Model for Fault Trees," Transactions of the American Nuclear Society, vol. 21, pp. 212-213, 1975.
44. H. E. Lambert, Measures of Importance of Events and Cut Sets in Fault Trees, UCRL-75853, Lawrence Livermore Laboratory, Livermore, CA, October 1974.
45. J. E. Kelly et al., "Sensitivity Assessments for Reactor Safety Studies," Transactions of the American Nuclear Society, vol. 21, pp. 342-343, 1975.

APPENDIX A

SIMPLIFIED ILLUSTRATION OF THE TO/THROUGH TECHNIQUE

FOR FAULT TREE CONSTRUCTION

FIGURE A.1. Barrier Configuration for Simplified Example of the To/Through Technique for Fault Tree Construction

FIGURE A.2. Fault Tree Representing Release from the Barrier System of the Preceding Figure. The analysis has been simplified by assuming 1) all radioactive material is initially contained within barrier 1; 2) the transport paths 2a→3a, 2a→3b, 2b→3a, and 2b→3b are all identical; and 3) the transport paths 1→2a and 1→2b are identical.

APPENDIX B

THE ACORN CODE FOR PLOTTING FAULT TREES

APPENDIX B

THE ACORN CODE FOR PLOTTING FAULT TREES

Fault trees at PNL are drawn by a CALCOMP plotter, using a tape created by the ACORN code. Trees can contain AND, OR, and INHIBIT gates. Basic events are plotted as diamonds, circles, or houses.

Gates share a common numbering system of no more than 4 digits with an A prefix. Basic events share a similar numbering system with an X prefix. The prefix and number appear on the plot within the symbol for each component. A rectangle atop each symbol contains a descriptive label for the component. In conformance with common practice for a multiply-appearing gate, takeoff and input triangles (transfers out and in, respectively) are used. The gate prefix and number appear within the triangle.

Tree logic is input as a series of Fortran logic statements. From these statements, the gate type and the components input to it can be determined. The descriptive labels are read in separately. Control parameters, additional input to help identify the types of basic events, and special numerical instructions, if needed, complete the input.

ACORN develops the logic structure of the tree from the input statements. The tree's physical structure is calculated from this logic structure. The latter is unalterable, but the former can be changed by a gate-lowering option, thereby materially improving the diagram's compactness and readability.

Although the code performs no analysis other than that needed for the plot, it provides other services. Input data are checked and diagnostics are provided. A printer plot of the tree is provided, showing the components by number in their relative locations on the final plot. The text of the descriptive labels is broken into lines. Finally, the logic input is optionally revised and punched in a format compatible with the input requirements of codes FAULT and FAULTG (Appendix F).

At present, ACORN is limited to 500 gates and 1000 total appearances of gates and events, but this limit can readily be increased. The maximum number of characters in a descriptive label is 75.

Running time is approximately linear with the number of components appearing on the plot. A tree with 200 components requires about 30 sec on the Cyber 74; one with 600 components, about 100 sec.

APPENDIX C

EQUATIONS FOR EVALUATING CUT SET AND TOP EVENT PROBABILITIES

APPENDIX C

EQUATIONS FOR EVALUATING CUT SET AND TOP EVENT PROBABILITIES

This appendix describes the probability equations used in the fault tree analysis codes FAULT and FAULTG. The equations assume independence of basic events within a cut set. Modifications for the case of dependent events are given in Appendix I. Other assumptions are discussed below.

C.1 INTRODUCTION

Two quantities are of prime interest in quantitative probability evaluation of fault trees. The first is the probabilities of certain individual cut sets. This information indicates the relative importance of cut sets in their contributions to the occurrence of the top event.

The second quantity is the probability of the top event of the tree or of the major branch. In the present risk-based analysis of fault trees, this quantity is generally less important because the risk, not the probability, of the top event is of interest. Calculation of the risk of the top event requires use of code RAFT, in addition to a fault tree analysis code.

The probability of the top event is conservatively approximated by the sum of the probabilities of all the cut sets.^(1,2,3) For rare events, the approximation is quite accurate.

The task of finding the second quantity of interest encompasses that of the first. The failure probability of each cut set is required. This is the probability that all basic events of a given cut set coexist at some time during the mission period.

A computer code or other means is assumed available to identify all the cut sets of a fault tree or major branch which survive the chain length cutoff. Repeated cut sets (those described differently on the tree but having the same collection of basic events) and repeated basic events within a cut set will have been eliminated. Cut sets will have the following appearance: X_1 , X_3X_5 , $X_9X_{11}X_{42}$, etc. Each X_i is a basic event

(circle or diamond), inhibit condition, house (on-switch), or off-switch. It is also assumed that suitable data or estimates are available for the basic events, inhibit conditions, etc.

Equations to evaluate the failure probabilities of cut sets are discussed in C.2. Much of the material is drawn from Reference 1. Discussions there regarding basic assumptions are generally not repeated. C.3 applies the equations in a form suitable for computer use.

C.2 EQUATIONS FOR EVALUATION OF CUT SET PROBABILITY

C.2.1 All Nonrepairable Components

If all of the n components in a cut set are nonrepairable, P (defined as the probability of failure for that cut set in the time interval from zero to t) is given by the exponential distribution

$$P = (1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t}) \dots (1 - e^{-\lambda_n t})$$

where λ_i = failure rate of component i , assumed constant in the time interval from zero to t (failures are also considered random and independent).

t = operating time or mission time.

If $\lambda t \ll 1$, then $(1 - e^{-\lambda t})$ can be replaced by λt with very little error. The small probability approximation, which will be used throughout the remainder of this Appendix, is always conservative. The above equation becomes

$$P = \lambda_1 t \lambda_2 t \dots \lambda_n t. \quad (1)$$

For computing P , all one-component cut sets are considered to be nonrepairable. The computing scheme of Section C automatically accomplishes this.

C.2.2 All Repairable Components

If all (or even several) of the n components in a cut set are repairable, a general solution is not practical because of complexities involving maintenance schedules, backup configurations, etc. However, a simplified treatment for cut set failure probability, assuming all $\lambda_{oi} t \ll 1$ and yielding steady-state, asymptotic values, uses

$$P = Q_2 Q_3 \dots Q_n \lambda_{o_1} t + Q_1 Q_3 \dots Q_n \lambda_{o_2} t + \dots + Q_1 Q_2 \dots Q_{n-1} \lambda_{o_n} t \quad (2)$$

where

λ_{o_i} = operating failure rate of component i
 Q_i = unavailability of component i, defined as the probability of being in a failed state when required, or as the expected fraction of the time that the component is down.

Values of Q_i for Equation (2) are given in Equations (3) and (4).

It is assumed that the Q_i are independent and that not all components in a cut set can be simultaneously disabled for maintenance and/or testing.

For an on-line component, one whose fault is typically the event

$$Q_i = \lambda_{o_i} \tau_i + \frac{t_{T_i}}{t_{TI_i}} + \frac{t_{M_i}}{t_{MI_i}} \quad \text{for } \lambda_{o_i} \tau_i \ll 1 \quad (3)$$

where

λ_{o_i} = operating failure rate

$\tau_i = \tau_{D_i} + \tau_{R_i}$ = average duration time of the fault

τ_{D_i} = average time to detect failure*

* If the component is not monitored, but is periodically tested, $\tau_D = t_{TI}/2$.
 If the component is monitored (annunciated), as well as periodically tested, the following expression⁽⁴⁾ is recommended:

$$\tau_D = \tau_{D_G} Q_G + \tau_{D_{NG}} (1 - Q_G)$$

where

τ_{D_G} = average time to detect component failure if the monitor functions

Q_G = availability of the monitor

$\tau_{D_{NG}}$ = average time to detect component failure if the monitor does not function.

In many cases, $\tau_{D_{NG}} = t_{TI}/2$.

τ_{R_i} = average time to repair a failure, once detected
 t_{T_i} = average test downtime (some components can be tested on-line, in which case $t_{T_i} = 0$)
 t_{TI_i} = average interval between tests
 t_{M_i} = average maintenance downtime
 t_{MI_i} = average maintenance interval.

Here and in Equation (3) the timing of maintenance and of testing among components in the same cut set is considered random, so that the Q_i are independent.

A standby component is one which is not on-line (and generally not operating) until demanded. All repairable components can be considered either on-line or standby, but not both. Thus the two categories are all-encompassing as well as mutually exclusive. For a standby component, one whose fault is typically the event.

Q_i comprises contributions originating prior to the demand (uncorrected failures; test; and maintenance) and those occurring at the demand (startup transients, etc.).

$$Q_i = \lambda_{s_i} \tau_i + Q_{d_i} + \frac{t_{T_i}}{t_{TI_i}} + \frac{t_{M_i}}{t_{MI_i}} \quad \text{for } \lambda_{s_i} \tau_i \ll 1 \quad (4)$$

where τ_i , t_{T_i} , t_{TI_i} , t_{M_i} , and t_{MI_i} are as used previously,

λ_{s_i} = standby failure rate (related to a standby component failing before it is demanded). λ_{s_i} may or may not equal λ_{o_i} . If the standby component is kept operating (but not on-line), λ_{s_i} often equals λ_{o_i} .

Q_{d_i} = the probability of component i failing to function on demand, given that it was capable of functioning immediately prior to the demand.*

C.2.3 Additional Considerations

Equations (1) - (4) are the basic results for evaluation of cut sets. However, several considerations, discussed below, necessitate adjustments to these equations.

C.2.3.1 Special Considerations for Standby Components

Consider a two-member cut set X_1X_2 , where component 1 is on-line and component 2 is its standby. The failure probability of cut set X_1X_2 consists of two terms: The first term represents the probability of (on-line) component 1 failing during the mission multiplied by the probability that (standby) component 2 is unavailable when demanded. The second term consists of three factors representing the situation in which component 1 fails, then component 2 comes on-line but fails before component 1 is repaired. The failure probability of cut set X_1X_2 can be shown to be

$$P = Q_2 \lambda_{o_1} t + (\lambda_{o_1} t)(1-Q_2)(\lambda_{o_2} \tau_1)$$

if $\lambda_{o_1} t$ and $\lambda_{o_1} \tau_1$ are both $\ll 1$. Assuming $(1-Q_2) \approx 1$ and rearranging,

$$P = Q_2 \lambda_{o_1} t + Q_1 \lambda_{o_2} t$$

where

Q_2 is given by Equation (4)

and $Q_1 = \lambda_{o_1} \tau_1$.

The result is identical to that using Equation (2) with Q_1 input as $\lambda_{o_1} \tau_1$.

We neglect maintenance and testing contributions to Q_1 in the above equation for P because failure of an on-line component constitutes a

* In many data sources λ_{s_i} , τ_i and Q_{d_i} are combined.

hazardous situation until repair is completed. It is also assumed that an on-line component and its standby are always connected by an AND gate and therefore always appear together in a cut set. This avoids the possibility of Q_i being called upon to assume different values in different cut sets.

C.2.3.2 Mixed Cut Sets

If m of the n components in a cut set are nonrepairable, Equation (2) is modified so that the factor $\frac{1}{m}$ ($m \neq 0$) multiplies each additive term whose $\lambda_{o_i} t$ represents a nonrepairable component.* Thus, in general, m of the n additive terms in Equation (2) would be multiplied by this factor. It can be shown that the remaining $n-m$ additive terms are each multiplied by the factor $\frac{1}{m+1}$. These $n-m$ terms are those whose $\lambda_{o_i} t$ represents a repairable component.

It is noted that the unavailability Q_i for a nonrepairable component i is $\lambda_i t$. Also, it is assumed that all $\tau_i \ll t$.

Example - given the cut set $X_1 X_2 X_3 X_4$
where X_1, X_3, X_4 are nonrepairable.

Thus $n = 4, m = 3$.

Equation (2) gives

$$P = Q_2 Q_3 Q_4 \lambda_1 t + Q_1 Q_3 Q_4 \lambda_2 t + Q_1 Q_2 Q_4 \lambda_3 t + Q_1 Q_2 Q_3 \lambda_4 t.$$

This result is adjusted by $\frac{1}{m} = \frac{1}{3}$ for terms involving λt of a non-repairable component. The term involving $\lambda_2 t$ is adjusted by $\frac{1}{m+1} = \frac{1}{4}$. The result is

$$P = \frac{1}{3} Q_2 Q_3 Q_4 \lambda_1 t + \frac{1}{4} Q_1 Q_3 Q_4 \lambda_2 t + \frac{1}{3} Q_1 Q_2 Q_4 \lambda_3 t + \frac{1}{3} Q_1 Q_2 Q_3 \lambda_4 t.$$

* Precise analysis shows that, for unequal λ_i , these factors differ from $\frac{1}{m}$. However, the sum of the m factors is still unity, and the overall probability of the cut set is unchanged.

C.2.3.3 Allowed Outage Times

If $\tau_{\max}$ is the maximum allowed outage time without propagating a failure sequence, then for each component i with this condition the factor

$$f_i = P(\tau_{D_i} + \tau_{R_i} > \tau_{\max_i}) = e^{-\tau_{\max_i} / (\tau_{D_i} + \tau_{R_i})} \quad (5)$$

is applied to every such Q_i or $\lambda_{o_i}t$ appearing in Equation (2). In some cases, more than one component within a cut set may have such a factor. If m of the n components in the cut set have such factors, then each of the n additive terms in Equation (2) will have m multiplicative f -factors. Extreme values of the f -factor exponent can cause misleading results. In such cases, more basic treatment of event probability is preferred.

C.2.3.4 Inhibit Conditions, Houses, and Switches

Term X_i of a cut set may represent an inhibit condition to term X_j with an inhibit fraction k (where $0 < k < 1$). If all components in the cut set are nonrepairable, then the factor k multiplies $\lambda_j t$ in Equation (1). If there are ℓ such inhibit conditions in the cut set, there will be ℓ multiplicative k -values in Equation (1). For cut sets of repairable components, the factor k (where k is an inhibit fraction for X_j) multiplies each $\lambda_j t$ and Q_j , for each additive term in Equation (2). If there are ℓ inhibit conditions in the cut set, there will be ℓ multiplicative k -values in each additive term of Equation (2). From a more mechanistic viewpoint, an inhibit condition can be accommodated in Equation (2) by setting $\lambda_{o_i} = 0$ and $Q_i = k$.

If term X_i of a cut set is a house (condition which is always present, an "on switch" with a probability of one), an analogous approach is used. Then $\lambda_{o_i} = 0$ and $Q_i = 1$ in Equation (2). The opposite "off switch" condition of zero probability is handled by setting $\lambda_{o_i} = 0$ and $Q_i = 0$.

C.3 USE OF THE EQUATIONS

In this section, a simplified method for evaluating the failure probability of a cut set is derived from the foregoing equations.

C.3.1 Input Requirements

For each basic event X_i in a cut set, the following quantities are input:

$P_i = \lambda_{oi} t$. Do not confuse P_i with P . The latter quantity is the probability for the entire cut set.

Q_i from Equation (3) for on-line repairable components or from Equation (4) for standby repairable components. For non-repairable components, $Q_i = P_i$.

$$m_i = \begin{cases} 0 & \text{if } X_i \text{ is repairable} \\ 1 & \text{if } X_i \text{ is nonrepairable.} \end{cases}$$

Recall that for an on-line component with a standby, $Q_i = \lambda_{oi} \tau_i$. For an inhibit condition, $P_i = 0$, $Q_i = k$, $m_i = 0$. For a house or switch, $P_i = 0$, $Q_i = 0$ or 1 , $m_i = 0$.

If a propagation delay factor f_i from Equation (5) is desired, both the P_i and Q_i values should be multiplied by $f_i (< 1)$ before being input. If there is no propagation delay, $f_i = 1$.

C.3.2 Calculational Procedure

For an n -term cut set $X_1 X_2 \dots X_n$, with

$$m = m_1 + m_2 + \dots + m_n = \sum_{i=1}^n m_i,$$

the following n products, each of n terms, are formed:

$$P(1) = Q_2 Q_3 \dots Q_n P_1$$

$$P(2) = Q_1 Q_3 Q_4 \dots Q_n P_2$$

$$P(3) = Q_1 Q_2 Q_4 \dots Q_n P_3$$

$\vdots$

$$P(n) = Q_1 Q_2 \dots Q_{n-1} P_n.$$

The notation used is that of Roberts.⁽⁵⁾

If $m = 0$, the cut set probability is

$$P = P(1) + P(2) + \dots + P(n).$$

For the case of $m \neq 0$, a multiplicative factor must be applied:

If $m_1 = 1$, then

$$P(1) = \frac{1}{m} P(1).$$

If $m_1 = 0$, then

$$P(1) = \frac{1}{m+1} P(1)$$

If $m_2 = 1$, then

$$P(2) = \frac{1}{m} P(2)$$

If $m_2 = 0$, then

$$P(2) = \frac{1}{m+1} P(2)$$

⋮

If $m_n = 1$, then

$$P(n) = \frac{1}{m} P(n)$$

If $m_n = 0$, then

$$P(n) = \frac{1}{m+1} P(n)$$

where the equality signs on the right are to be interpreted as "is replaced by," rather than "is equal to." The former expression is the interpretation used in computer operations.

The cut set probability is again

$$P = P(1) + P(2) + \dots + P(n).$$

C.3.3 Sample Calculations

Given the cut set $X_1X_2X_3X_4$.

- a. All input events represent failures of repairable components.

Input:	Event	P_i	Q_i	m_i
	X_1	P_1	Q_1	0
	X_2	P_2	Q_2	0
	X_3	P_3	Q_3	0
	X_4	P_4	Q_4	0

Output:

$$m = 0 + 0 + 0 + 0 = 0$$

$$P(1) = Q_2Q_3Q_4P_1$$

$$P(2) = Q_1Q_3Q_4P_2$$

$$P(3) = Q_1Q_2Q_4P_3$$

$$P(4) = Q_1Q_2Q_3P_4$$

$$P = P(1) + P(2) + P(3) + P(4)$$

- b. All input events nonrepairable

Input:	Event	P_i	Q_i	m_i
	X_1	P_1	Q_1	1
	X_2	P_2	Q_2	1
	X_3	P_3	Q_3	1
	X_4	P_4	Q_4	1

Note: For nonrepairable components $P_i = Q_i$

Output:

$$m = 1 + 1 + 1 + 1 = 4$$

$$P(1) = \frac{1}{4} Q_2Q_3Q_4P_1$$

$$P(2) = \frac{1}{4} Q_1 Q_3 Q_4 P_2$$

$$P(3) = \frac{1}{4} Q_1 Q_2 Q_4 P_3$$

$$P(4) = \frac{1}{4} Q_1 Q_2 Q_3 P_4$$

Since

$$Q_1 = P_1$$

$$Q_2 = P_2$$

$$Q_3 = P_3$$

$$Q_4 = P_4$$

$$P = P_1 P_2 P_3 P_4$$

c. Events X_2 and X_3 nonrepairable, X_1 and X_4 repairable

Input:	<u>Event</u>	<u>P_i</u>	<u>Q_i</u>	<u>m_i</u>
	X_1	P_1	Q_1	0
	X_2	P_2	Q_2	1
	X_3	P_3	Q_3	1
	X_4	P_4	Q_4	0

Output:

$$m = 2$$

$$P(1) = \frac{1}{3} Q_2 Q_3 Q_4 P_1$$

$$P(2) = \frac{1}{2} Q_1 Q_3 Q_4 P_2$$

$$P(3) = \frac{1}{2} Q_1 Q_2 Q_4 P_3$$

$$P(4) = \frac{1}{3} Q_1 Q_2 Q_3 P_4$$

The above equations could be simplified, since $P_2 = Q_2$ and $P_3 = Q_3$.

$$P = P(1) + P(2) + P(3) + P(4)$$

- d. Events X_1, X_2, X_4 repairable. X_3 is an inhibit condition to X_4 with probability k , where $0 < k < 1$.

Input:	<u>Event</u>	<u>P_i</u>	<u>Q_i</u>	<u>m_i</u>
	X_1	P_1	Q_1	0
	X_2	P_2	Q_2	0
	X_3	0	k	0
	X_4	P_4	Q_4	0

Output:

$$m = 0$$

$$P(1) = Q_2 k Q_4 P_1$$

$$P(2) = Q_1 k Q_4 P_2$$

$$P(3) = 0$$

$$P(4) = Q_1 Q_2 k P_4$$

$$P = P(1) + P(2) + P(3) + P(4)$$

$$= P(1) + P(2) + P(4)$$

- e. Same as 4, except that X_3 is a house (on-switch)

Input: same, except $Q_3 = 1$

Output: same, except k is replaced by 1.

- f. Events X_1, X_3 repairable. X_2 represents a repairable standby component to X_1 . X_4 represents a repairable standby component to X_3 .

Input:	<u>Event</u>	<u>P_i</u>	<u>Q_i</u>	<u>m_i</u>
	X_1	P_1	$Q_1 = \lambda_{o1} \tau_1$	0
	X_2	P_2	Q_2	0
	X_3	P_3	$Q_3 = \lambda_{o3} \tau_3$	0
	X_4	P_4	Q_4	0

Output:

$$m = 0$$

$$P(1) = Q_2 Q_3 Q_4 P_1$$

$$P(2) = Q_1 Q_3 Q_4 P_2$$

$$P(3) = Q_1 Q_2 Q_4 P_3$$

$$P(4) = Q_1 Q_2 Q_3 P_4$$

$$P = P(1) + P(2) + P(3) + P(4)$$

- g. Events X_1, X_3 nonrepairable. X_2 represents a repairable standby component to X_1 . X_4 represents a repairable standby component to X_3 .

Input	Event	$\frac{P_i}{Q_i}$	$\frac{Q_i}{P_i}$	$\frac{m_i}{P_i}$
	X_1	P_1	Q_1	1
	X_2	P_2	Q_2	0
	X_3	P_3	Q_3	1
	X_4	P_4	Q_4	0

Output:

$$m = 2$$

$$P(1) = \frac{1}{2} Q_2 Q_3 Q_4 P_1$$

$$P(2) = \frac{1}{3} Q_1 Q_3 Q_4 P_2$$

$$P(3) = \frac{1}{2} Q_1 Q_2 Q_4 P_3$$

$$P(4) = \frac{1}{3} Q_1 Q_2 Q_3 P_4$$

The above equations could be simplified since $P_1 = Q_1$, and $P_3 = Q_3$.

$$P = P(1) + P(2) + P(3) + P(4).$$

C.4 REFERENCES

1. USAEC, Reactor Safety Study, An Assessment of Accident Risks in Commercial Nuclear Power Plants, WASH-1400 Draft, August 1974.

2. W. E. Vesely, Analysis of Fault Trees by Kinetic Tree Theory, IN-1330, Idaho Nuclear Corporation, Idaho Falls, ID, October 1969.
3. H. Lambert, Fault Tree Analysis: An Overview, UCRL-75904, Lawrence Livermore Laboratory, Livermore, CA, August 1974.
4. D. F. Haasl, "Fault Tree Analysis," course notes, Joint Center for Graduate Study, Richland, WA, February 1974, to be published in book form.
5. N. H. Roberts, "Systems Safety Analysis," course notes, University of Washington, Seattle, WA, 1975.

APPENDIX D

DETERMINING THE EVENT CHAIN LENGTH CUTOFF, n_{cut}

APPENDIX D

DETERMINING THE EVENT CHAIN LENGTH CUTOFF, n_{cut}

D.1 REVIEW OF CUT SET PROBABILITY EQUATIONS

The following assumptions are made: 1) A_{cut} has been calculated; 2) the tree consists of, at most, inhibit conditions (including houses) and AND and OR gates; 3) a list is available of P_i , Q_i and m_i values (probability, unavailability, and repairability, see Appendix C) for all basic events.

Nonrepairable components are described by the quantities P_{NR_i} , $Q_{NR_i} = P_{NR_i}$, and $m_i = 1$. Repairable components are described by P_{R_i} , Q_{R_i} , and $m_i = 0$. Inhibit conditions are described by $P_{I_i} = 0$, $Q_{I_i} = k_i$, and $m_i = 0$.

For a cut set of n nonrepairable components,

$$(1)^* A_{NR} = P_{NR_1} P_{NR_2} \dots P_{NR_n} \quad (1 \text{ additive term})$$

For a cut set of n repairable components,

$$(2) A_R = Q_{R_1} Q_{R_2} \dots Q_{R_{n-1}} P_{R_n} + Q_{R_1} Q_{R_2} \dots Q_{R_{n-2}} Q_{R_n} P_{R_{n-1}} + \dots \\ + Q_{R_2} Q_{R_3} \dots Q_{R_n} P_{R_1} \quad (n \text{ additive terms})$$

For a mixed cut set, with m nonrepairable and $(n-m)$ repairable components, the result of (2) is adjusted to A_M by applying factors of $\frac{1}{m}$ to additive terms containing P_{NR} and $\frac{1}{m+1}$ to additive terms containing P_R .

With p inhibits in a cut set containing $(n-p)$ other basic events

$$(3) A_I = k_1 k_2 \dots k_p \left(Q_{p+1} Q_{p+2} \dots Q_{n-1} P_n + Q_{p+1} Q_{p+2} \dots Q_{n-2} Q_n P_{n-1} \right. \\ \left. + \dots + Q_{p+2} Q_{p+3} \dots Q_n P_{p+1} \right) \quad (n-p \text{ additive terms})$$

* Cut set probability, represented by the symbol P in Appendix C, is represented by A here because the discussion relates to probability terms appearing in Equation (1) of the main report. It is hoped that no confusion results.

because $P_{I_i} = 0$ for an inhibit gate. The additive terms in (3) may be multiplied by factors of $\frac{1}{m}$ and $\frac{1}{m+1}$ as appropriate, if m nonrepairable components appear in the cut set.

D.2 ASSIGNING n_{cut}

From a given set of P_i and Q_i data, it is not obvious which type of cut set--all repairable components, all nonrepairable, or mixed--yields the largest value of A for a given n . These limiting A values produce the upper bound sequence $A_{\text{ub}}(n)$ for determination of n_{cut} . No simple yet precise solution is apparent. However, an approximate solution can be obtained. The solution is approximate in that, while it does furnish an upper bound on $A(n)$, the numbers may be much larger than the least upper bound $A_{\text{lub}}(n)$, which is the actual maximum value of A for a given n . The calculated value of n_{cut} may thus be too conservative (large). The saving in computer time might not be so great as with a more accurate estimation of $A_{\text{ub}}(n)$.

Equations (1) through (3) can be represented by a general form for all types of components described previously:

$$(4) A = z_1 Q_2 Q_3 \dots Q_n P_1 + z_2 Q_1 Q_3 Q_4 \dots Q_n P_2 + \dots \\ + z_n Q_1 Q_2 \dots Q_{n-1} P_n \quad (n \text{ additive terms})$$

Here $z_i = 1$ if $m = 0$; if $m \neq 0$, $z_i = \frac{1}{m}$ or $\frac{1}{m+1}$ as appropriate. If event i is an inhibit condition, $P_i = 0$. For p inhibit conditions, the n additive terms reduce to $(n-p)$ additive terms.

Define

$$(5) A^+(n) \equiv n \text{ Max}_{\text{all } Q} (Q_1 Q_2 \dots Q_{n-1}) P_{\text{max}} \geq A(n)$$

where the Q_i may include the k_i of inhibit conditions.

$A^+(n)$ is thus an upper bound on $A(n)$ for all types of cut sets consisting of n (or more) unique events. This statement may be verified by

checking the expression for $A^+(n)$ against Equations (1)-(3). Obviously, $A^+(n) \geq A_R(n)$ because of the maximizing of Q and P values. $A^+(n) > A_M(n)$ for the same reason and because of the factors of $\frac{1}{m}$ and $\frac{1}{m+1}$ in the latter. $A_{NR}(n)$ is actually a special case of $A_M(n)$ with $m = n$. $A^+(n) > A_I(n)$ by similar reasoning and by the fact that $n > (n-p)$.

In summary, $A^+(n)$ is found by forming the product of n, of the largest P value among the basic events, and of the largest (n-1) values of Q_i . The sequence $A^+(1), A^+(2), \dots$ is generated until, for some n, $A^+(n) \leq A_{cut}$. This value of n is called n_{cut} . Cut sets of $\geq n_{cut}$ terms can be discarded.

D.3 AN EXAMPLE DEMONSTRATING THE METHOD

The method was applied to data from the WFP preliminary fault tree for water basin storage of solidified waste. Basic events of highest probability and unavailability are listed in Table D.1. The highest P_i and Q_i (and k_i for inhibit conditions) entries have been numbered in sequence by the circled digits.

With $A^+(n)$ from Equation (5) as an upper bound, the following sequence is generated by forming the products of the numbered entries in succession. Event X_{70} constitutes P_{max} and has a value of 0.3.

$$\begin{aligned} A^+(1) &= (1) (0.3) &&= 3 \times 10^{-1} \\ A^+(2) &= (2) (0.1) (0.3) &&= 6 \times 10^{-2} \\ A^+(3) &= (3) (0.1) (0.1) (0.3) &&= 9 \times 10^{-3} \\ &\vdots \\ A^+(10) &= (10) (0.1)^8 (0.04) (0.3) &&= 1.2 \times 10^{-9} \\ A^+(11) &= (11) (0.1)^8 (0.04) (0.01) (0.3) &&= 1.3 \times 10^{-11} \end{aligned}$$

Since A_{cut} for this tree was shown in 7.4.2 to be 2.3×10^{-11} , $A^+(11) < A_{cut}$ and all cut sets of ≥ 11 components may be discarded.

D.4 IMPROVED METHODS FOR ASSIGNING n_{cut}

The ultimate objective is to reduce $A_{ub}(n)$ as much as possible, so that $A_{ub}(n)$ becomes $\leq A_{cut}$ for the smallest n possible. The constraint is that $A_{ub}(n) \geq A(n)$ for every n-event cut set.

TABLE D.1. Basic Events of Highest Probability and Unavailability in the Preliminary Water Basin Storage Fault Tree

Event Type	Event Number	P_i	Q_i
Repairable	X_{70}	① 0.3	10^{-3}
	X_{309}	② 0.2	2×10^{-5}
	X_{80}	③ 0.15	10^{-3}
	X_{139}	0.09	10^{-3}
	X_{311}	0.09	10^{-3}
	X_{102}	0.09	10^{-5}
	X_8	10^{-2}	10^{-3}
	X_{267}	10^{-2}	10^{-3}
	X_{306}	10^{-2}	10^{-3}
	X_{103}	10^{-2}	10^{-5}
Nonrepairable	X_{54}	0.1	① 0.1
	X_{291}	10^{-2}	⑩ 10^{-2}
	X_{298}	4×10^{-3}	4×10^{-3}
	X_{289}	10^{-3}	10^{-3}
	X_{290}	10^{-3}	10^{-3}
	X_{292}	10^{-3}	10^{-3}
Inhibit	X_{235}	0	② 0.1
	X_{240}	0	③ 0.1
	X_{66}	0	④ 0.1
	X_{253}	0	⑤ 0.1
	X_{296}	0	⑥ 0.1
	X_{297}	0	⑦ 0.1
	X_{307}	0	⑧ 0.1
	X_{124}	0	⑨ 0.04
	X_6	0	⑪ 10^{-2}
	X_{312}	0	⑫ 10^{-2}

At worst, obtaining a closer bound on A involves trial-and-error assembly of combinations of high probability events according to Equations (1)-(3). However, several shortcuts simplify the process. For example, one can sometimes show that two basic events of relatively high probability never appear in the same cut set. The most rigorous way to demonstrate this is to show that the events are mutually exclusive. In the water basin tree, coexistence of basic events X_{307} and X_{124} (see Table D.1) would require the

basin covers to be on and off the basin simultaneously.* Thus, X_{124} (the lower probability event) may be deleted from any hypothetical cut set including X_{307} ; the event of next lower probability replaces X_{124} .

With this shortcut and use of the more precise Equation (3), an improved upper bound for the probability of 10-term cut sets can be found:

$$A_{ub}(10) = (0.1)^7 \left[\frac{10^{-3} 10^{-2} (0.1)}{2} + \frac{10^{-3} (0.1) 10^{-2}}{2} + \frac{10^{-2} (0.1) (0.3)}{3} \right] = 1.01 \times 10^{-11}$$

for events numbered 235, 240, 66, 253, 296, 297, 307, 70, 54, 291. Thus, $n_{cut} = 10$ and all cut sets of ≥ 10 unique terms may be discarded.

It is seen that, as more effort is expended, the successively more accurate values generated for A_{ub} , for a given value of n , come closer to A_{lub} . Involved is a trade-off of manual calculation time against the saving in computer time achieved by using the smallest justifiable value of n_{cut} .

* The precise wording for these two basic events is such that they are not strictly complementary.

APPENDIX E

TREATMENT OF ABSORPTION

APPENDIX E

TREATMENT OF ABSORPTION

E.1 INTRODUCTION^(1,2)

A fault tree is a logic diagram depicting component failures and other fault events that can produce system failure through AND and OR combinatorial logic. It is a binary model, convertible to a probabilistic model by means of Boolean algebra.

In addition to commutative, associative and distributive laws, Boolean algebra includes two types of laws which particularly affect the identity and summation of cut sets derived from AND ($\cap$) and OR ($\cup$) operations. These are the idempotent laws (identities),

$$X \cap X = X \quad (1)$$

and

$$X \cup X = X, \quad (2)$$

and the law of absorption,

$$X \cap (X \cup Y) = X \quad (3)$$

and

$$X \cup (X \cap Y) = X. \quad (4)$$

Equations (1), (2) and (4) are relevant to this discussion.

E.2 APPLICATION OF THE IDENTITY LAWS

Cut sets identified in the analysis of a fault tree may contain repeated basic events. Such cut sets are not minimal cut sets. An example is the cut set $X_1 X_1 X_7 X_{42}$. In accordance with the first identity law, Equation (1), such cut sets are treated by code FAULT or FAULTG (with a second check by code RAFT) to remove redundant events. The example cut set would become $X_1 X_7 X_{42}$; event X_1 need occur only once in the sequence to result in system failure.

Analysis of a fault tree may result in repeated cut sets. Again, such a group of cut sets is not minimal because one cut set is a subset of another cut set (namely, an identical cut set). An example is the following collection: $X_1X_7X_{42}$, $X_1X_7X_{42}$. In accordance with the second identity law, Equation (2), such collections are treated by code RAFT to delete repeated cut sets. (The deletion can also be performed by FAULTG, but only partially performed by FAULT.) Thus the example collection of cut sets would become simply $X_1X_7X_{42}$.

E.3 TRADITIONAL APPLICATION OF THE ABSORPTION LAW

Equation (4) shows that, if one cut set in the collection representing the tree is a proper (nonidentical) subset of another cut set, then, by the absorption law of Boolean algebra, the longer cut set may be deleted. The following cut set collection provides an example: X_1X_7 , $X_1X_7X_{42}$. The total probability understood for the two cut sets is $P(X_1X_7\bar{X}_{42}) + P(X_1X_7X_{42})$, where $\bar{X}_{42}$ is the complement of X_{42} . Recall that

$$P(A \cap B) = P(A) \cdot P(B|A) \quad (5)$$

where the event A is now taken to be X_1X_7 . The total probability becomes

$$P(X_1X_7\bar{X}_{42}) + P(X_1X_7X_{42}) = P(X_1X_7) [P(\bar{X}_{42}|X_1X_7) + P(X_{42}|X_1X_7)] = P(X_1X_7), \quad (6)$$

since the events X_{42} and $\bar{X}_{42}$ are disjoint and their total probability is unity. Thus, in accordance with the absorption law, the second cut set may be deleted. We may think of this process in the following way: events X_1 , X_7 , and X_{42} are not all required simultaneously for system failure; only X_1 and X_7 are required simultaneously.

E.4 USE OF FAULT TREES IN RISK ANALYSIS

The above approach is traditional in fault tree analysis and is generally incorporated in related computer codes. The viewpoint is that the sole numerical measure of the events comprising a fault tree is that of event

probability. As long as the sole numerical result sought from the fault tree is probability, the approach is satisfactory.

Fault trees, however, are playing an increasing role in risk analysis. Risk is defined here as the probability of an event multiplied by a numerical measure of the consequences of the event. Thus the significance of the top event of a fault tree used directly in risk analysis is no longer limited solely to probability. A second measure, the consequences, is equally important. Furthermore, it can be demonstrated that the consequences associated with the top event are propagated upward through the tree by the consequences associated with many of the basic events in the tree.

The more intimately the consequences for each event of a release sequence can be coupled with the probability of the event, the more accurate will be the resulting representation of the system. If consequences are not considered in the fault tree analysis and if failure sequences are screened on the basis of probability alone, sequences involving small probability but large consequences (and possibly large risk) may be mistakenly deleted.

E.5 THE POTENTIAL FOR ABSORPTION ERRORS

One way that such an error could occur is through injudicious absorption. Theoretically, if the consequence measure is the average consequence of the sequence, absorption presents no problems. Practically, however, unless information is available concerning its distribution over all relevant circumstances, the average consequence may be difficult to compute. In the example of E.3, consequence calculations when only X_1 and X_7 occur may be straightforward. But event X_{42} might radically increase the consequences, a relevant circumstance easily overlooked if absorption is injudiciously applied. The next section shows how to calculate the magnitude of this type of error.

An example of this type of basic event is the failure of a spray system for removal of radioactive material from the atmosphere within a contaminated nuclear facility. Spray system failure is not essential for release of radioactive material from the facility, so cut sets containing this basic

event would not be minimal cut sets. However, this event could greatly increase the quantity of material released to the environment. Only an actual calculation can compare the risk considering spray system failure against that without it.

E.6 THE MAGNITUDE OF POTENTIAL ABSORPTION ERRORS IN FAULT TREE ANALYSIS USED DIRECTLY IN RISK STUDIES

The magnitude of the potential errors noted in E.5 can be evaluated. Let S be the underlying sample space, P the associated probability measure, and c the consequence. If S is partitioned into n disjoint subsets S_i , so that $S = \bigcup_{i=1}^n S_i$, it can be shown that the risk is

$$R = \sum_{i=1}^n P(S_i) E(c_i | S_i). \quad (7)$$

That is, the risk can be computed by partitioning the sample space into disjoint events, finding the conditional expected consequence given the event, multiplying by the probability of the event, and then summing.

The meaning of $E[c_i | S_i]$ is important. Suppose S_i is made up of discrete points $s_{i1}, \dots, s_{im}$. In this case

$$E(c_i | S_i) = \sum_{j=1}^m c_{ij} P(s_{ij} | S_i). \quad (8)$$

That is, the expected consequence of an event is the weighted average of the consequence over all possible circumstances leading to the event's occurrence.

The role of fault tree analysis when used directly in risk studies is to aid in identifying a meaningful collection of sets S_i and in evaluating P for those sets. The top event is the union of all sets with significant consequences. Ideally, the top event is broken down into disjoint (or near disjoint) sets of clear physical interpretation (minimal cut sets). Probabilities are assigned to each of the minimal cut sets, and the probability of the top event is taken to be the sum of the probabilities of

the cut sets. This is exact if the cut sets are disjoint; otherwise the small probability approximation is applied to yield a conservative estimate.

The absorption problem for fault trees used in risk analysis is not exactly that an event of small probability and large consequence is omitted. More precisely, it is that the expected consequence is incorrectly specified.

The cut sets $(X_1X_7, X_1X_7X_{42})$, discussed previously, provide an illustration. Picking up the analysis from Equation (6), we let $c(1,7,42)$, $c(1,7,\overline{42})$, and $c(1,7)$ be the consequences of $X_1X_7X_{42}$, $X_1X_7\overline{X}_{42}$, and X_1X_7 , respectively. Then

$$\begin{aligned}
 c(1,7) &= P(X_1X_7X_{42}|X_1X_7) \cdot c(1,7,42) \\
 &\quad + P(X_1X_7\overline{X}_{42}|X_1X_7) \cdot c(1,7,\overline{42}) \\
 &= P(X_{42}|X_1X_7) \cdot c(1,7,42) + P(\overline{X}_{42}|X_1X_7) \cdot c(1,7,\overline{42}) \\
 &= P(X_{42}|X_1X_7) \cdot c(1,7,42) + [1-P(X_{42}|X_1X_7)] \cdot c(1,7,\overline{42}) \\
 &= c(1,7,\overline{42}) + P(X_{42}|X_1X_7) [c(1,7,42) - c(1,7,\overline{42})]. \quad (9)
 \end{aligned}$$

The proper estimate of risk is

$$\begin{aligned}
 R &= P(X_1X_7)\{c(1,7,\overline{42}) + P(X_{42}|X_1X_7)[c(1,7,42) - c(1,7,\overline{42})]\} \\
 &= P(X_1X_7) c(1,7,\overline{42}) + P(X_1X_7X_{42})[c(1,7,42) - c(1,7,\overline{42})]. \quad (10)
 \end{aligned}$$

The practical difficulty comes in applying this equation after the absorption law has been used. The only cut set appearing in the output would be X_1X_7 . The analyst would likely use $c(1,7,\overline{42})$, instead of $c(1,7)$ from Equation (9), as the expected consequence of X_1X_7 . This leads to an underestimated risk,

$$R^- = P(X_1 X_7) \cdot c(1, 7, \overline{42}), \quad (11)$$

which is sometimes seriously in error.

For simplicity, the conservative present method calls for retaining both cut sets $X_1 X_7$ and $X_1 X_7 X_{42}$. This leads to a (generally small) overestimate of risk. In this case, the overestimated risk R^+ of the two cut sets would be

$$R^+ = P(X_1 X_7) \cdot c(1, 7, \overline{42}) + P(X_1 X_7 X_{42}) \cdot c(1, 7, 42). \quad (12)$$

In the detailed analysis phase, the proper estimate R would be determined.

General expressions for the errors of R^- and of R^+ are now derived. Given two cut sets E_1 and E_2 , with $E_2 \subset E_1$, the absorption law states that only E_1 should be retained. If this approach is injudiciously followed, the result is

$$R^- = P(E_1) \cdot c(1). \quad (13)$$

If both cut sets are retained,

$$R^+ = P(E_1) \cdot c(1) + P(E_2) \cdot c(2). \quad (14)$$

As is seen from Equation (10), the proper risk estimate is

$$\begin{aligned} R &= [P(E_1) - P(E_2)] \cdot c(1) + P(E_2) \cdot c(2) \\ &= P(E_1) \cdot c(1) + P(E_2) \cdot c(2) - P(E_2) \cdot c(1). \end{aligned} \quad (15)$$

The fractional error of R^- is

$$\frac{R - R^-}{R} = \frac{P(E_2) [c(2) - c(1)]}{P(E_1) \cdot c(1) + P(E_2) \cdot c(2) - P(E_2) \cdot c(1)}. \quad (16)$$

The fractional error of R^+ is

$$\frac{R^+ - R}{R} = \frac{P(E_2) c(1)}{P(E_1) c(1) + P(E_2) c(2) - P(E_2) c(1)} \quad (17)$$

Potential release sequences reported in Reference 2 illustrate the above concepts. Table E.1 presents the results of calculating R , R^+ , and R^- for a number of pairs of sequences. The upper member of each pair is the minimal sequence and has the higher probability. The lower, nonminimal sequence of each pair has consequences greater than (or equal to) those of the upper sequence. The errors of R^+ and of R^- are given.

TABLE E.1. Potential Release Sequences⁽²⁾ Demonstrating Possible Absorption Errors in Fault Tree Analysis Used Directly for Risk Studies

Pair of Sequences	Probability, yr ⁻¹	Consequences, man-rem (x10 ⁶)	Risk, R, man-rem (x10 ⁶)yr ⁻¹	$\frac{R^+ - R}{R} \times 100, \%$	$\frac{R - R^-}{R} \times 100, \%$
AD- α	2-8 ^(a)	1.4			
ACD- α	5-11	2.8	2.807-8	0.25	0.25
AF- δ	1-8	1.4			
AHF- δ	2-10	3.1	1.434-8	2.0	2.4
AH- ϵ	1-6	1.3-4			
ACHF- ϵ	1-7	7.5-3	8.67-10	1.5	85
S ₁ D- β	3-8	0.07			
S ₁ CD- β	1-10	0.29	2.122-9	0.33	1.0
S ₂ D- ϵ	9-6	1.3-4			
S ₂ CD- ϵ	2-8	7.5-3	1.317-9	0.20	11
TML- α	3-8	1.4			
TMLB'- α ^(b)	3-8	2.8	8.4-8	50	50
TKQ- α	3-8	1.4			
TKMQ- α	1-8	1.4	4.2-8	33	0

a. Abbreviated scientific notation is used throughout this table. Thus 2 - 8 means 2×10^{-8} .

b. The probability of B' is somewhat less than unity, but roundoff led to a listed probability identical to that of the shorter sequence.

It is seen that injudicious absorption can lead to calculated risks much less than those calculated with consequence-weighted absorption. The proposed R^+ treatment (elimination of absorption) generally leads to a smaller error, is always conservative, and saves computer time.

The risk analysis approach of Reference 2 used fault trees indirectly (to obtain branch probabilities for event trees). Such an approach is not vulnerable to the error of consequence underestimation described here. (In fact, the Reference 2 calculations are of the R^+ type.) However, a direct fault tree approach for risk analysis, such as the present one, would be vulnerable to this type of error if absorption were used injudiciously.

E.7 EFFECTS ON CODES FAULT, FAULTG, AND RAFT

The identity and absorption treatments affect the event chain length cutoff, as mentioned in 7.4.3 of the main report. In applying a cutoff, n_{cut} , on chain length, a cut set with $\geq n_{cut}$ events might be identified. If one or more events in the cut set were repeated, the cut set might be mistakenly discarded. This is because such a cut set with $\geq n_{cut}$ events would reduce to one with $< n_{cut}$ events after redundant events were eliminated. For this reason, codes FAULT and FAULTG continually check for repeated event indices, according to Equation (1), as they work through the logic of the tree. The check for repeated indices precedes the comparison of chain length n against n_{cut} , thereby eliminating the possibility of the above error. Thus, the n_{cut} value is applied only against unique events in a developing cut set.

As mentioned in E.2, duplicate cut sets are eliminated by codes RAFT, FAULTG, and FAULT (only partial treatment in FAULT).

Because of the demonstrated pitfalls related to cut set absorption in risk analysis, no absorption of the type shown in Equation (4) is performed for preliminary evaluations in the present techniques. Later detailed analysis of cut sets will include correction of R^+ by means of Equation (15).

Elimination of absorption implies that no cut set can disappear by absorption with a shorter cut set according to Equation (4). This procedure overstates the risk, but the effect is generally very small.

Absorption checking typically is responsible for a large fraction of the running time of codes which identify cut sets. Deletion of this operation significantly reduces the running time of such codes. On the other hand, the number of cut sets carried along is increased because nonminimal cut sets are not eliminated. However, screening based on n_{cut} then on A_{cut} greatly reduces the number of cut sets; thus there is still a major reduction in overall computer time.

E.8 REFERENCES

1. G. Birkhoff and S. MacLane, A Survey of Modern Algebra, Revised edition, MacMillan Company, New York, 1953.
2. USAEC, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, draft, August 1974.

APPENDIX F

INPUT/OUTPUT DESCRIPTION FOR FAULT TREE ANALYSIS CODES FAULT AND FAULTG

APPENDIX F

INPUT/OUTPUT DESCRIPTION FOR FAULT TREE ANALYSIS CODES FAULT AND FAULTG

F.1 CODE FAULT

F.1.1 Input Format

FAULT requires that each logic gate and component be given an alphanumeric name. To simplify cut set identification and handling, component names must be one character and an integer presently not to exceed 512. Gate names are not restricted and can consist of up to seven alphanumeric characters. One card is read for each logic gate in the tree. The card contains the gate name, type of gate (AND, OR), number of gates input to it, number of components input to it, and names of the gates and components. Each component and gate is internally indexed and placed in Fortran logic arrays. Along with this tree description, control information and component failure data are input.

FAULT input consists of the following groups:

Title Card	
Control Information	(* DATA)
Tree Description	(* TREE)
Component Failure Data	(* RATES).

The first card of the case is the title card and can contain 80 columns of case identification. The beginning of each group of information following the title is indicated by a special control card of the form *KEYWORD beginning in Column 1. The end of each group of information is indicated by a special control card END starting in Column 1. An example of the deck is shown below with each input section described in detail.

Title Card

* DATA

(Control Data)

END

* TREE

(Logic Description)

END

* RATES

(Rate Data)

END

* DATA (two cards)

Card 1 (A10, 6I5, E10.0)

<u>Variable</u>	<u>Columns</u>	<u>Description</u>
ITOPTR	1-6	Name of gate which is the desired top of the tree for calculation (default: logic top of the tree).
JTMAX	11-15	Maximum cut set size program will identify. JTMAX presently limited to 10 or less.
IFP1	16-20	Edit option of unordered cut sets 0 No print or write to Tape 9 1 Write to Tape 9 only 2 Print only 3 Print and write to Tape 9
IFP2	21-25	Edit option of ordered cut sets 0 No print or write to Tape 9 1 Write to Tape 9 only 2 Print only 3 Print and write to Tape 9

Card 1 (A10, 6I5, E10.0) (contd)

<u>Variable</u>	<u>Columns</u>	<u>Description</u>
IFP3	26-30	Edit option minimal cut sets (not active)
IFP4	31-35	Edit option of predicted cut sets algorithm -X print predicted cut sets for each gate by size up to size X for the entire tree 0 no print X print predicted cut sets for the specified and/or actual top gate up to size X.
IYCODE	36-40	0 omit probability calculation 1 perform probability calculation
THRESH	41-50	Value of probability cut-off

Card 2 (2A5, 5X, A8)

NOGO	1-5	NOGOB edit data only DEFAULT: perform calculation
XPUNCH	6-10	PUNCH: punch cards for *TREE block in FORTRAN logical order DEFAULT: no cards punched
NORATE	16-23	NOBRATES read only *RATE and END card for block *RATE DEFAULT: read block *RATE

*TREE (one card for each gate in the tree)
(A8, A3, 10X, 2I1, 2X, 6A8, A6)

GATE (1, J)	1-6	Gate name
GATE (2, J)	9-11	Gate type (AND, OR)
NGG (J)	22	Number of input gates
NCC (J)	23	Number of input components
GATE (3, J)	26-31	Input gate or component
GATE (4, J)	34-39	Input gate or component
GATE (5, J)	42-47	Input gate or component

*TREE (one card for each gate in the tree) (contd)
(A8, A3, 10X, 211, 2X, 6A8, A6)

<u>Variable</u>	<u>Columns</u>	<u>Description</u>
GATE (6, J)	50-55	Input gate or component
GATE (7, J)	58-63	Input gate or component
GATE (8, J)	66-71	Input gate or component
GATE (9, J)	74-79	Input gate or component

*RATES (one card for each component)
(A7, 20X, I3, 3E12.4)

NAM (J)	1-6	Component name
MODE (J)	28-30	0 repairable component 1 nonrepairable component
PROB (J)	31-42	Probability of component
UNAV (J)	43-54	Unavailability of component
FACTX	55-66	Multiplier for PROB (J) and UNAV (J) Default: 1

F.1.2 Output

FAULT output includes these sections: 1) the input control information and user options; 2) the fault tree logic description; 3) the ordered fault tree; 4) the ordered tree for the specified top (option); 5) the predicted number of cut sets and their size for each gate of the fault tree (option); 6) the input probability data; 7) the cut set disposition table; 8) the cut sets and their probabilities ordered by cut set length (option).

Also, an unformatted tape or disk file can be created which contains the cut sets and their probabilities in blocks of one hundred. This tape can be input into RAFT or used for further processing of the cut sets.

F.1.3 Limitations

FAULT can presently handle the logic of AND and OR gates. With the use of the probability equations in Appendix C, houses and inhibit gates can also be modeled. The code is presently set up for trees of up to 200 logical gates and 250 events. The capacity of FAULT is about 4×10^5 cut sets retained (surviving the two cutoffs), although running time would be restrictive at this upper range. Depending on the efficiency of the screening process, fault trees one to two orders of magnitude larger than 4×10^5 BICS can be accommodated.

F.2 CODE FAULTG

F.2.1 Input Format

Except for the *DATA section, the FAULTG input sections and their order are identical to those described for FAULT. The differences in the *DATA section are outlined below:

*DATA (two cards)

Card 1 (A10, 615, E10.0, 215)

<u>Variable</u>	<u>Columns</u>	<u>Description</u>
ITOPTR	1-6	Name of gate which is the desired top of the tree for calculations (default: logical top of the tree)
JTMAX	11-15	Maximum cut set size program will identify (JTMAX presently limited to 10 or less)
IFP1	16-20	Edit option cut set disposition for each gate 0 no disposition information printed 1 cut set disposition for each gate printed.
IFP2	21-25	Maximum number of cut sets printed. If number of cut sets greater than IFP2 no printing of cut sets.
IFP3	26-30	Edit option minimal cut sets (not active)

Card 1 (A10, 6I5, E10.0, 2I5) (contd)

<u>Variable</u>	<u>Columns</u>	<u>Description</u>
IFP4	31-35	Edit option of predicted cut set algorithm. -X print predicted cut sets for each gate by size up to size X for the entire tree 0 no print X print predicted cut sets for the speci- fied top gate and/or the actual top gate by size up to size X (X presently limited to 20)
IYCODE	36-40	0 omit probability calculation 1 perform probability calculation
THRESH	41-50	Value of probability cut-off
IWEED	51-55	0 performs check for duplicate cut sets 1 omits check for duplicate cut sets
IPROBD	56-60	0 no file created 1 file of the top gate cut sets not surviving the cut-offs is created

Card 2 is identical to that for FAULT.

F.2.2 Output

Output includes 1) the input control information and user options; 2) the fault tree logic description; 3) the ordered fault tree; 4) the ordered tree for the specified top; 5) the predicted number of cut sets and their size for each gate of the fault tree (option); 6) the input probability data; 7) the cut set disposition table for each gate (option); and 8) the cut sets and their probabilities ordered by cut set length (option).

In addition, an unformatted tape or disk file can be created which contains the gate name, the cut sets, and their probabilities in blocks of one hundred. This tape can be input into RAFT or used for further processing of the cut sets.

F.2.3 Limitations

FAULTG can presently handle the logic of AND and OR gates. With the use of the probability equations in Appendix C, houses and inhibit gates can be modeled. The code is presently set up for 400 gates and 512 events. The capacity of FAULTG is about 4×10^5 cut sets retained, although running time would be restrictive at this upper range. Depending on the efficiency of the screening process, fault trees one to two orders of magnitude larger than 4×10^5 BICS can be accommodated.

APPENDIX G

INPUT/OUTPUT DESCRIPTION OF CODE RAFT FOR CALCULATION OF RELEASE
QUANTITY AND RISK MEASURE

APPENDIX G

INPUT/OUTPUT DESCRIPTION OF CODE RAFT FOR CALCULATION OF RELEASE QUANTITY AND RISK MEASURE

G.1 INPUT

Detailed input instructions appear in Table G.1.

The maximum number of events per cut set is currently 10. The maximum number of entries in the table of release fraction versus conditional probability is currently 4. The additive contributors (described in Subsection 7.6.2.3) to the risk measure of a cut set are termed sub-cut sets.

Thus, if a cut set contains 10 events, each with four entries in the distributed release fraction table, there will be $4^{10} = 1.05 \times 10^6$ individual risk measure computations for the cut set. Each such computation will generate a sub-cut set. The calculational effort obviously becomes enormous unless restraint is exercised in the use of distributed release fractions.

RAFT can either use cut set probabilities obtained from another source (e.g., FAULT or FAULTG) or calculate the probabilities itself by the equations of Appendix C.

G.2 OPERATION

Hash addressing as a function of event sequence is used to determine redundancy of cut sets. RAFT continues by accessing a single cut set and computing the individual risk measures. A maximum of the 37 largest values of risk measure are retained per cut set for a line printer. However, the combined total of the risk measure values is retained for the cut set and for the entire major branch.

Two threshold values can be applied to determine the relative significance of each cut set. The first is the probability cutoff which, as in FAULT and FAULTG, could eliminate the cut set entirely. The second is a risk threshold for sub-cut sets in order to minimize the printed output from each cut set. A cut set print limit is also available to minimize the total number of cut sets for the output printer file. The number of sub-cut sets printed is the minimum of these two factors and the limit of 37 mentioned previously. Because difficulties could arise if the risk threshold is chosen too high, the code prints at least two sub-cut sets.

Two independent quantities contributing to the total risk-measure sum are calculated. One sum is related to cut sets which have components output on the printer. The other, the "branch residual sum," represents that part of the major branch which had no components listed as output. The "branch residual sum" is helpful in determining the relevance of the risk threshold.

G.3 OUTPUT

Cut sets are numbered and listed according to descending value of risk measure. In addition, the cumulative risk fraction is printed to indicate the cut sets contributing most to the total risk measure of the major branch. The total risk measure is given at the end of the run.

The numerical designations of the events within each cut set are printed along with the verbal descriptions of the events. The cut set probability is also printed.

For each printed sub-cut set, the contributing values of the release fractions for each event are printed. The probability of the sub-cut set is also given.

G.4 LIMITATIONS

RAFT places no limit on the number of input cut sets. However, the output file is limited to 8000 cut sets for each value of the number of events per cut set. That is, 8000 cut sets having one event, 8000 having two events, etc. If this limit is exceeded, the overrun cut sets are handled on disk scratch file. However, a large increase in running time results.

TABLE-G.1. Input Instructions

C*****

C
C B N W P R O G R A M R A F T
C (RISK ASSESSMENT FOR FAULT TREES)

C
C INPUT INSTRUCTIONS*

C VARIABLE TYPE DESCRIPTION
C -----

C
C DRAFT

C TIA= REAL TOTAL INVENTORY AVAILABLE.
C PRESET TIA=1.0

C CUTOFA= REAL CUTSET PROBABILITY THRESHOLD.
C PRESET CUTOFA=0.

C CUTOFF= REAL RISK THRESHOLD.
C PRESET CUTOFF=0.

C FIELD= INTEGER CARD INPUT FIELD DEFINITION.
C PRESET FIELD=80

C LUDISK= INTEGER DISC DEVICE USED FOR RANKING RELEASE FRACTIONS.
C PRESET LUDISK=1

C MEDIA= ALPHANUMERIC SOURCE OF CUTSET MEDIA.
C ="DISK", CUTSETS WILL BE READ FROM DISC USING
C A NON-FORMATTED READ TO OBTAIN (N,P,INDICE(I))
C WHERE N=THE NUMBER OF EVENTS/CUTSET
C P=CUTSET PROBABILITY
C INDICE=NUMERIC INDEX FOR EACH EVENT.

C ="CARDS", CUTSETS WILL BE READ FROM CARDS USING
C A FORMATTED READ TO OBTAIN (N,P,INDICE(I))
C SUCH AS (12,E10.0,1015) FOR EACH CUTSET.
C PRESET MEDIA="DISK"

C DEBUG= ALPHANUMERIC DECISION FLAG FOR PRINTING HASHED CUTSETS.
C ="YES", TABLE OF HASHED CUTSETS IS PRINTED.
C ="NO", NO TABLE IS PRINTED.
C PRESET DEBUG="NO"

C MODIFY= ALPHANUMERIC DECISION FLAG TO RE-COMPUTE AND OVERLOAD CUTSET
C PROBABILITIES.
C ="NO", CUTSET PROB. ARE THOSE INPUT VIA MEDIA.
C ="YES", CUTSET PROB. ARE COMPUTED USING PQ(I,J),
C AND MODF(J) DESCRIBED BELOW.
C PRESET MODIFY="NO"

C CUTSET= INTEGER RESTART VALUE AVAILABLE FOR DEFINING CUTSET
C NUMBER WHEN MULTIPLE CASE EXECUTION IS REQUIRED.
C PRESET CUTSET=1

C TREES= REAL RESTART VALUE AVAILABLE FOR CONTINUING THE RISK
C SUM WHEN MULTIPLE CASE EXECUTION IS REQUIRED.
C PRESET TREES=0.

C TITLE= ALPHANUMERIC CASE TITLE, SINGLE CARD RECORD AVAILABLE FOR
C ALPHANUMERIC DESCRIPTION.
C PRESET TITLE=" " "


```

C RF(1,1)= REAL      RF(I,J),I=1,4/J=1,500 RELEASE FRACTIONS.
C                    J.LE.(1+RELEASE FRACTIONS/EVENT).LE.4
C                    J=1,500 INDEX USED TO DEFINE THE EVENT.
C                    PRESET RF(1,J)=0. AT START OF EACH RUN.
C                    NOT PRESET FOR SUBSEQUENT CASES WITHIN A RUN.
C
C CP(1,1)= REAL      CP(I,J),I=1,4/J=1,500 CONDITIONAL PROBABILITIES.
C                    ONE-TO-ONE CORRESPONDANCE WITH RF(I,J).
C                    1.LE.(1+CONDITIONAL PROB./EVENT).LE.4
C                    J=1,500 INDEX USED TO DEFINE THE EVENT.
C                    PRESET CP(1,J)=0. AT START OF EACH RUN.
C                    NOT PRESET FOR SUBSEQUENT CASES WITHIN A RUN.
C
C MODE(1)= INTEGER   REPAIRABLE OR NON-REPAIRABLE COMPONENT FLAG.
C                    MODE(J),J=1,500 EVENTS.
C                    =0, EVENT COMPONENT IS REPAIRABLE.
C                    =1, EVENT COMPONENT IS NON-REPAIRABLE.
C                    NOT REQUIRED UNLESS MODIFY="YES"
C                    NOT PRESET.
C
C PQ(1,1)= REAL      PQ(I,J),I=1,2/J=1,500 EVENTS.
C                    I=1 DEFINES EVENT COMPONENT PROBABILITY.
C                    I=2 DEFINES EVENT COMPONENT UNAVAILABILITY.
C                    NOT REQUIRED UNLESS MODIFY="YES"
C                    NOT PRESET.
C
C LIMIT= INTEGER     LIMIT.LE.37
C                    MAXIMUM ALLOWABLE LINE LIMIT PER CUTSET.
C                    PRESET LIMIT=25
C
C HSHING= ALPHANUMERIC DECISION FLAG TO INITIATE HASHING ALGORITHM TO
C                    DETERMINE CUTSET REDUNDANCY.
C                    =YES, HASHING ALGORITHM IS INITIATED.
C                    =NO, HASHING ALGORITHM IS NOT USED,
C                    EVENT SEQUENCES ARE NOT ORDERED.
C                    REPEATED EVENTS WITHIN A CUTSET ARE NOT CHECKED,
C                    AND RFT IS NOT INPUT CUTSET LIMITED.
C                    PRESET HSHING="YES"
C
C MAXWRT= INTEGER     MAXIMUM NUMBER OF CUTSETS FOR THE PRINT FILE.
C                    1.LE.MAXWRT.LE.2000
C                    PRESET MAXWRT=2000
C
C READ INTEGER        INPUT FLAG USED TO INDICATE HOLLERITH DEFINITIONS.
C                    =YES, ACORN CARDS ARE READ TO DESCRIBE EVENTS.
C                    IN ADDITION, COLUMNS 3,4,5 ARE READ TO DEFINE
C                    CORRESPONDANCE BETWEEN EVENTS AND HOLLERITH DATA
C                    A 7/8/9 CARD IS EXPECTED AFTER EACH GROUP.
C                    =NO, ACORN CARDS ARE NOT EXPECTED AS INPUT.
C                    PRESET READ="NO"
C
C PRINT= INTEGER      OPTION FLAG FOR PRINTING HOLLERITH INPUT.
C                    =YES, ALL EVENTS WILL BE DEFINED ON OUTPUT.
C                    =NO, NO EVENTS WILL BE DEFINED ON OUTPUT.
C                    PRESET PRINT="NO"
C
C GATE= ALPHANUMERIC FLAG TO INDICATE PRESENCE OF GATE NAME ON DISK
C                    INPUT FILE.
C                    PRESET GATE="YES"
C
C $
C *****

```

APPENDIX H

SPECIALLY CONSTRUCTED FAULT TREE FOR TESTING CODES FAULT, FAULTG, AND RAFT

H.1

APPENDIX I

MATHEMATICAL TREATMENT OF DEPENDENT EVENTS IN FAULT TREE ANALYSIS

APPENDIX I

MATHEMATICAL TREATMENT OF DEPENDENT EVENTS
IN FAULT TREE ANALYSIS

I.1 INTRODUCTION

Events feeding into a common logic gate on a fault tree are often not independent of one another. Such dependencies have been discussed in References 1 to 3, but only defining equations were presented. Furthermore, some of the terminology was potentially confusing.

Section I.2 treats dependent events more thoroughly although in its present form it relates to nonrepairable components only. The reader not interested in mathematical detail should proceed to Section I.3. There the dependency equations are summarized for convenient use in hand calculations. The equations are also recast into simple forms for use with computer codes such as FAULT and FAULTG.

Two cases of dependence will be analyzed. In Model I, components ultimately fail due to independent causes, but the failure of one component may affect the failure rates of others. An example is two pumps operating in parallel. Failure of one pump increases the load on the other and may increase its failure rate.

In Model II, failures are due to (generalized) shocks or stresses, affecting more than one component simultaneously. An example is two components near a steam line. Rupture of the line could simultaneously disable both components.

In what follows, "dependence" will refer to stochastic (statistical) dependence. Confusion may result if statistical dependence and physical dependence are not distinguished. For instance, the notion of one-sided dependency refers to a physical dependence, for there is no such thing as one-sided statistical dependence. For event A to be (statistically) dependent on event B, it is not necessary that a physical mechanism exist such that B partially causes A. Moreover, there is no way in which A can (statistically) depend on B, yet B be (statistically) independent of A.

I.2 THEORY

The analysis is most conveniently carried out in the time domain. The event A is defined as component A failing prior to some mission time T.

Thus, if T_A is the time of failure of component A, then

$$A = \{T_A \leq T\}.$$

The two dependency models will be discussed separately. Treated will be components A and B whose failure events are connected logically through AND or OR gates. Extension to more than two components will be indicated.

I.2.1 Dependency Model I

The dependency here arises from the fact that component A may have one failure rate when component B is operating, and another when B is in the failed state. The situation is similar for component B. It is assumed that the conditional failure densities are available.

I.2.1.1 Treatment of AND Gates

Events A and B are regarded as inputs to an AND gate, an intersection operation. In the time domain,

$$A \cap B = \{T_A \leq T, T_B \leq T\}.$$

From basic probability theory,⁽⁴⁾ let $E_1, \dots, E_k$ be a collection of events such that

$$E_i \cap E_j = \emptyset, \text{ the empty set} \\ i \neq j$$

and

$$\sum_{i=1}^k P(E_i) = 1.$$

Then for any event C,

$$P(C) = \sum_{i=1}^k P(C|E_i).$$

Here $P(C|E_i)$ represents the conditional probability of event C, given event E_i .

Applying this result,

$$P(T_A \leq T, T_B \leq T) = P(T_A \leq T, T_B \leq T | T_A < T_B) \cdot P(T_A < T_B) \\ + P(T_A \leq T, T_B \leq T | T_B < T_A) \cdot P(T_B < T_A). \quad (1)$$

If $E_1 = \{T_A < T_B\}$ and $E_2 = \{T_B < T_A\}$, the above can be written as

$$P(A \cap B) = P(A \cap B | E_1) P(E_1) + P(A \cap B | E_2) P(E_2). \quad (2)$$

The utility of Equation (1) is that direct evaluation of $P(A \cap B)$ requires knowledge of the (unknown) joint density of T_A and T_B , but Equation (1) can be evaluated in terms of the conditional densities.⁽⁵⁾ The latter are generally easier to formulate from physical reasoning. Expressions are now needed for terms of the form

$$P(T_A \leq T, T_B \leq T | T_A < T_B) \quad (3)$$

and

$$P(T_A < T_B). \quad (4)$$

The conditional densities are taken to be independent of the failure times. This assumption can often be justified physically and is equivalent to an exponential life distribution.

To evaluate Equation (3), assume A fails before B, and let T_{A1} be the time of A's failure, and T_{B2} be the time from the failure of A to the failure of B. Also, let f_{A1} and f_{B2} be the probability density functions of T_{A1} and T_{B2} , respectively. Then

$$P(T_A \leq T, T_B \leq T | T_A < T_B) = P(T_{A1} + T_{B2} \leq T) \\ = \int_0^T \int_0^t f_{A1}(t-u) f_{B2}(u) du dt \\ = \int_0^T [f_{A1} * f_{B2}](t) dt, \quad (5)$$

where $[f_{A1} * f_{B2}]$ represents the convolution of f_{A1} and f_{B2} .

To evaluate Equation (4), let f_{B1} be the conditional density of T_B , given that component A has not failed. Then

$$P(T_A < T_B) = \int_0^{\infty} f_{A1}(t) \int_0^t f_{B1}(u) du dt. \quad (6)$$

This method may be extended to more than two components without conceptual difficulty. However, the computation required increases rapidly because the family of conditioning events corresponds to all possible permutations of failure time sequences. For instance, with three events A, B, and C, the conditioning events are

$$E_1 = \{T_A < T_B < T_C\}$$

$$E_2 = \{T_A < T_C < T_B\}$$

$$E_3 = \{T_B < T_A < T_C\}$$

$$E_4 = \{T_B < T_C < T_A\}$$

$$E_5 = \{T_C < T_A < T_B\}$$

$$E_6 = \{T_C < T_B < T_A\}.$$

Example 1: Assume components A and B operate in parallel and exhibit exponential failure densities, e.g., $f_A = \lambda_A e^{-\lambda_A t}$. Component A operates initially with failure rate λ_{A1} and with failure rate λ_{A2} when component B fails. Define λ_{B1} and λ_{B2} similarly. Then

$$P(T_A \leq T, T_B \leq T | T_A < T_B) = 1 - \left[\frac{\lambda_{B2}}{\lambda_{B2} - (\lambda_{A1} + \lambda_{B1})} \right] e^{-(\lambda_{A1} + \lambda_{B1})T} - \left[\frac{\lambda_{A1} + \lambda_{B1}}{\lambda_{A1} + \lambda_{B1} - \lambda_{B2}} \right] e^{-\lambda_{B2}T}. \quad (6A)$$

Expanding Equation (6A) in a power series and truncating after the first nonzero term (assuming small probabilities) gives

$$P(T_A \leq T, T_B \leq T | T_A < T_B) \approx \frac{1}{2} \lambda_{B2} T [\lambda_{A1} T + \lambda_{B1} T]. \quad (6B)$$

From Equation (6),

$$P(T_A < T_B) = \frac{\lambda_{A1}}{\lambda_{A1} + \lambda_{B1}}. \quad (6C)$$

Similarly,

$$P(T_A \leq T, T_B \leq T | T_B < T_A) \approx 1/2 \lambda_{A2} T [\lambda_{A1} T + \lambda_{B1} T] \quad (6D)$$

and

$$P(T_B < T_A) = \frac{\lambda_{B1}}{\lambda_{A1} + \lambda_{B1}}. \quad (6E)$$

Multiplying (6B) by (6C) and (6D) by (6E) and then adding gives

$$P(A \cap B) \approx 1/2 \left[\lambda_{A1} T \lambda_{B2} T + \lambda_{A2} T \lambda_{B1} T \right]. \quad (6F)$$

It has been assumed that λ_{A1} and λ_{B1} are not greatly different in magnitude.

I.2.1.2 Treatment of OR Gates

An OR gate represents a union operation; its probability can be expressed in several ways. For Dependency Model I, the most useful expression is

$$P(A \cup B) = 1 - P(\bar{A} \cap \bar{B}), \quad (7)$$

where $\bar{A}$ represents the complement of event A. This expression is particularly easy to evaluate, since

$$\begin{aligned} P(\bar{A} \cap \bar{B}) &= P(A \text{ does not fail and } B \text{ does not fail}) \\ &= P(T_A > T \text{ and } T_B > T) \\ &= \int_T^\infty f_{A1}(u) \int_T^\infty f_{B1}(v) dv du. \end{aligned} \quad (8)$$

Example 2: Consider the same situation as in Example 1, but with the AND gate replaced by an OR gate. Then

$$P(\bar{A} \cap \bar{B}) = e^{-(\lambda_{A1} + \lambda_{B1})T},$$

so that

$$P(A \cup B) = 1 - e^{-(\lambda_{A1} + \lambda_{B1})T} \approx \lambda_{A1}T + \lambda_{B1}T. \quad (9)$$

It follows that low-probability failures of components A and B can be considered independent, as far as an OR gate is concerned. This is because the increased failure rate of one component following failure of the other component need not be realized to satisfy the "any input" requirement of the OR gate.

I.2.2 Dependency Model II

For this model of dependency, consider two components subject to a series of low-probability, but always fatal, shocks or peak stresses. An arriving shock can fail component A, or component B, or both A and B. Assume that the shocks occur according to three Poisson processes. Shocks failing only component A have rate parameter λ_A ; those failing only B, λ_B ; those failing both A and B, λ_{AB} . Then the joint distribution of T_A and T_B is given by⁽⁶⁾

$$\begin{aligned} \bar{F}(t_A, t_B) &= P(T_A > t_A, T_B > t_B) \\ &= \exp \left[-\lambda_A t_A - \lambda_B t_B - \lambda_{AB} \max(t_A, t_B) \right] \end{aligned} \quad (10)$$

where t_A and t_B are dummy variables.

The probability density function* is given by⁽⁷⁾

* The function $\bar{F}$ is not absolutely continuous with respect to (two-dimensional) Lebesgue measure; thus, strictly speaking, a density does not exist. However, it can be shown that there exists a measure μ , a mixture of one- and two-dimensional Lebesgue measure, such that f is the Radon-Nikodym derivative of F (not $\bar{F}$) with respect to μ . [Here $F = P(T_A \leq t_A, T_B \leq t_B)$.] Thus, the measure-theoretic difficulties can essentially be ignored.

$$f(t_A, t_B) = \begin{cases} \lambda_A(\lambda_B + \lambda_{AB}) \bar{F}(t_A, t_B), & t_B > t_A > 0 \\ \lambda_B(\lambda_A + \lambda_{AB}) \bar{F}(t_A, t_B), & t_A > t_B > 0 \\ \lambda_{AB} \bar{F}(t_A, t_B), & t_A = t_B > 0. \end{cases} \quad (11)$$

The common mode analysis of Reference 8 can be shown to be a special case of Model II with $\lambda_A = \lambda_B$ and $\beta \equiv \lambda_{AB}/(\lambda_A + \lambda_{AB})$, where β is the fraction of failures involving simultaneous failure of A and B.

I.2.2.1 Treatment of AND Gates

As with Model I, an expression for $P(A \cap B)$ is needed. With a joint density for T_A and T_B , this is obtained in the time domain:

$$\begin{aligned} P(A \cap B) &= P(T_A \leq T, T_B \leq T) = \int_0^T \int_0^T f(t_A, t_B) dt_A dt_B \\ &= 1 - e^{-(\lambda_A + \lambda_B + \lambda_{AB})T} - e^{-(\lambda_A + \lambda_{AB})T} - e^{-(\lambda_B + \lambda_{AB})T} \\ &\quad + (\lambda_A T)(\lambda_B T) + \lambda_{AB} T - \frac{\lambda_{AB}^2 T^2}{2}. \end{aligned} \quad (12)$$

The term $(\lambda_A T)(\lambda_B T)$ in Equation (12) can be interpreted as the probability of system failure due to components A and B failing from independent shocks. The term $\lambda_{AB} T$ represents the probability of system failure due to failure of components A and B from the same shock.

I.2.2.2 Treatment of OR Gates

Under Model II the failure times have exponential marginal densities, so

$$P(A) = 1 - e^{-(\lambda_A + \lambda_{AB})T}$$

$$P(B) = 1 - e^{-(\lambda_B + \lambda_{AB})T}$$

and

$$\begin{aligned}
 P(A \cup B) &= P(A) + P(B) - P(A \cap B) \\
 &= 1 - e^{-(\lambda_A + \lambda_B + \lambda_{AB})T} \\
 &\approx (\lambda_A + \lambda_B + \lambda_{AB})T \\
 &= P(A) + P(B^*)
 \end{aligned}$$

where B^* is the event {B fails from independent shock}.

I.2.2.3 Extension to Gates with More than Two Input Events

Extension to AND or OR gates with more than two input events is straightforward. In general a separate series of shocks must be postulated for every possible combination of events. Thus, the computational burden can increase rapidly. However, in applications, it may be that some (or most) combinations can be eliminated, resulting in considerable simplification.

For example, with three components A, B, and C, the most general model has a distribution given by

$$\begin{aligned}
 \bar{F}(t_A, t_B, t_C) &= P(T_A > t_A, T_B > t_B, T_C > t_C) \\
 &= \exp [-\lambda_A t_A - \lambda_B t_B - \lambda_C t_C - \lambda_{AB} \max(t_A, t_B) \\
 &\quad - \lambda_{AC} \max(t_A, t_C) - \lambda_{BC} \max(t_B, t_C) \\
 &\quad - \lambda_{ABC} \max(t_A, t_B, t_C)].
 \end{aligned}$$

If, however, there are no shocks common to components A and C, then

$$\begin{aligned}
 \bar{F}(t_A, t_B, t_C) &= \exp [-\lambda_A t_A - \lambda_B t_B - \lambda_C t_C - \lambda_{AB} \max(t_A, t_B) \\
 &\quad - \lambda_{BC} \max(t_B, t_C)].
 \end{aligned}$$

I.3 APPLICATION

I.3.1 Summary of Results for Manual Calculations

The equations derived above are suitable for detailed manual analysis of dependencies and are summarized below:

Dependency Model I

AND gate:

$$P(A \cap B) = P(A \cap B | E_1) P(E_1) + P(A \cap B | E_2) P(E_2) \quad (13)$$

$$E_1 = \{A \text{ fails before } B\}$$

$$E_2 = \{B \text{ fails before } A\}.$$

OR gate:

$$P(A \cup B) = 1 - P(\bar{A} \cap \bar{B}) \quad (14)$$

Dependency Model II

AND gate:

$$P(A \cap B) = P(A^*) P(B^*) + P(C) \quad (15)$$

$$A^* = \{A \text{ fails independently of } B\}$$

$$B^* = \{B \text{ fails independently of } A\}$$

$$C = \{A \text{ and } B \text{ fail due to same cause}\}.$$

OR gate:

$$P(A \cup B) = P(A) + P(B^*). \quad (16)$$

The time domain forms derived previously are used for evaluation of the individual terms in the probability equations.

I.3.2 Recasting into Simple Forms for Use with Existing Computer Codes

A simplified treatment of dependent events is required for use in the computerized screening phase of fault tree evaluation. The dependency

equations can be cast into the same form as the simplified probability equations for independent events, given in Appendix C. These equations are, for AND gates,

$$P(A \cap B) = P(A) \cdot P(B) \quad (17)$$

and, for OR gates with small probability inputs,

$$P(A \cup B) \cong P(A) + P(B). \quad (18)$$

The objective, then, is to cast the complex dependency results derived previously into the simplified forms of Equations (17) and (18).

I.3.2.1 Treatment of AND Gates

1. Dependency Model I. If exponential conditional densities are assumed, as in Example 1, then Equation (13) becomes

$$P(A \cap B) = 1/2 [\lambda_{A1} T \lambda_{B2} T + \lambda_{A2} T \lambda_{B1} T].$$

For independent events, the input to the computer codes involves terms of the form

$$P(A) = \lambda_{A1} T$$

and

$$P(B) = \lambda_{B1} T.$$

Using these terms we can write

$$\begin{aligned} P(A \cap B) &= 1/2 [P(A) P(B) \cdot \frac{\lambda_{B2}}{\lambda_{B1}} + P(A) P(B) \frac{\lambda_{A2}}{\lambda_{A1}}] \\ &= P(A) P(B) [1/2 (\lambda_{B2}/\lambda_{B1} + \lambda_{A2}/\lambda_{A1})]. \end{aligned} \quad (19)$$

Thus the term $P(B) [1/2 (\lambda_{B2}/\lambda_{B1} + \lambda_{A2}/\lambda_{A1})]$ can be substituted for $P(B)$ in Equation (17). The computer codes can thereby handle dependent events, while retaining the simple input format of Equation (17) for independent events.

2. Dependency Model II. Equation (15) can be rewritten as

$$P(A \cap B) = P(A^*) [P(B^*) + P(C)/P(A^*)]. \quad (20)$$

Thus $P(A^*)$ can be used for $P(A)$ and the bracketed term for $P(B)$, thereby allowing the form of Equation (17) to be retained.

I.3.2.2 Treatment of OR Gates

1. Dependency Model I. For exponential conditional densities, Equation (14) is approximately

$$P(A \cup B) \approx P(A) + P(B),$$

which is the form required for Equation (18).

2. Dependency Model II. From Equation (16),

$$P(A \cup B) = P(A) + P(B^*), \quad (21)$$

which has the form of Equation (18) with $P(B^*)$ substituted for $P(B)$.

In all cases it should be noted that if events A and B appear individually elsewhere in the fault tree, then the probability calculations in those locations may be upset by the alterations appearing in Equations (19), (20), and (21). A careful check is needed.

I.4 REFERENCES

1. D. F. Haasl, "Fault Tree Analysis," course notes, Joint Center for Graduate Study, Richland, WA, February 1974, to be published in book form.
2. H. E. Lambert, Systems Safety Analysis and Fault Tree Analysis, UCID-16238, Lawrence Livermore Laboratory, University of California, May 1973.
3. E. T. Rumble et al., Generalized Fault Tree Analysis for Reactor Safety, Science Applications, Inc. EPRI 217-2-2, June 1975.
4. R. B. Ash, Real Analysis and Probability, Academic Press, New York, 1972.
5. J. J. Eiss, "The Reliability of Dependent Parallel or Standby N-Unit Redundancies," Operations Research 5, 1968, pp. 1068-1083.
6. A. W. Marshall and I. Olkin, "A Multivariate Exponential Distribution," Journal of the American Statistical Assoc., vol. 62, pp. 30-44, March 1967.
7. B. M. Bemis et al., "Estimation and Hypothesis Testing for Parameters of a Bivariate Exponential Distribution," Journal of the American Statistical Assoc., vol. 67, pp. 927-929, December 1972.
8. K. N. Fleming, A Reliability Model for Common Mode Failures in Redundant Safety Systems, GA-A 13284, General Atomic Company, San Diego, CA, December 1974.

APPENDIX J

PREVIOUS APPROACHES TO THE COMPLETENESS PROBLEM

APPENDIX J

PREVIOUS APPROACHES TO THE COMPLETENESS PROBLEM

The completeness problem has been addressed by other investigators, either in developing generic siting criteria^(1,2) or in estimating the risk associated with a particular facility.⁽³⁾ Although the procedures used varied, the cited studies all invoked the same concepts. It was claimed⁽¹⁾ that the impossibility of identifying all possible accidents "may be surmounted by assuming that the fission product release is a continuous function of accident probability, i.e. that there is an infinite number of possible accidents. This assumption places a conservative upper limit on the risk."

We are indebted to the previous investigators for focusing attention on the completeness problem and for presenting helpful ideas in their approaches to the problem. However, we feel that their studies have not surmounted the problem because of certain unjustified or erroneous assumptions, as discussed below. Our own improved methods, building on their ideas, have not yet surmounted these difficulties and are not included in this report. Indeed, the problem is probably not solvable unless additional assumptions are made about the unknown sequences and/or the discovery process, as is done in Appendix K. Furthermore, there is no assurance that the methods in the cited studies place a conservative upper limit on the risk.

Contributing to the difficulties in the previous studies are loose usage and/or circular definitions of the words "probability," "probability density function," and "risk." Even the term "risk probability" appears in one title, adding to the confusion.

The approach used in the cited studies involves extension of Farmer's limit line concept.⁽⁴⁾ Farmer interpreted the limit line as an aid for deciding whether the risk of any single identified accident sequence is unacceptable. Use of the limit line or release envelope to represent a continuous spectrum of accidents departs from Farmer's original intent. Nor is

there any assurance that all possible accidents are correctly included. Furthermore, the apparent use of the probability versus consequences release envelope itself as the probability density function^(1,2) is mathematically incorrect:⁽⁵⁾ the two types of curves should not be confused. For example, one purported density function of Reference 2 integrates to a value considerably greater than unity; another, to a value much less than unity. Neither can be a density function. Integrating the density function of Reference 1 yields a risk about twice that of the risk sum for the nine points identified as representing specific potential LOCA accidents. Yet, there is no reason why this particular ratio should exist for that system: one cannot show that the ratio should in reality be any particular number. Only with assumptions concerning the number and nature of the unidentified points and/or concerning one's ability to find them can the value of the ratio be derived (subject to the assumptions made).

The techniques of Reference 3 are more technically satisfying but still involve questionable assumptions. In this case, a true density function was generated but was assumed to be log normal. It is highly unlikely that fitting the identified points with the density function will produce reasonable parameter estimates, considering the manner in which these points were generated.

The procedures of Reference 6, although only indirectly related to the completeness problem, appear to be valid for the problem studied. This is because overall (observed) system data for release versus frequency were treated, rather than specific release sequences being formulated.

REFERENCES

1. H. J. Otway and R. C. Erdmann, "Reactor Siting and Design from a Risk Viewpoint," Nuclear Engineering and Design, vol. 13, pp. 365-376, 1970.
2. M. Meleis and R. C. Erdmann, "The Development of Reactor Siting Criteria Based upon Risk Probability," Nuclear Safety, vol. 13, pp. 22-28, 1972.
3. H. J. Otway et al., "A Risk Estimate for an Urban-Sited Reactor," Nuclear Technology, vol. 12, pp. 173-184, 1971.
4. F. R. Farmer, "Reactor Safety and Siting: A Proposed Risk Criterion," Nuclear Safety, vol. 8, pp. 539-548, 1967.
5. L. V. Kimmel, The Expected Environmental Costs of Radiation-Release Accidents at the Trojan Nuclear Plant, ERC-5, Environmental Research Center, Washington State University, Pullman, WA, May 1973.
6. H. J. Otway et al., "A Method for Estimating the Risk from a Plowshare Detonation," Nuclear Technology, vol. 11, pp. 323-330, 1971.

APPENDIX K

TECHNIQUES FOR ESTIMATING THE ADDITIONAL RISK
REPRESENTED BY UNIDENTIFIED SEQUENCES

APPENDIX K

TECHNIQUES FOR ESTIMATING THE ADDITIONAL RISK REPRESENTED BY UNIDENTIFIED SEQUENCES

This appendix presents several techniques for estimating the additional risk represented by unidentified release sequences of the type discussed in Section 8.3.4.2. Of course, the results depend directly on the assumed characteristics of the unidentified sequences. However, it is instructive to observe the effects of different assumptions on the magnitude of the estimated risk.

K.1 PROBLEM STATEMENT

Consider the collection of all possible release sequences of a system as a large, but finite, set Ω with an unknown number of elements, N . At some point in time after extensive study, n such (disjoint or low-probability) sequences have been identified:

$$\{\omega_1, \dots, \omega_n\} \subset \Omega.$$

From this subset the calculated risk is

$$R_c = \sum_{i=1}^n r(\omega_i).$$

The risk for each $\omega \in \Omega$ is defined as

$$r(\omega) = p(\omega) c(\omega).$$

Here $p(\omega)$ is the probability of the failure sequence and $c(\omega)$ is the consequence of its occurrence.

The actual risk of the system, which is not known, is

$$R_a = \sum_{\omega \in \Omega} r(\omega) = \sum_{i=1}^N r(\omega_i), \quad (1)$$

where

$$\Omega = \{\omega_1, \dots, \omega_N\}.$$

Clearly $N \geq n$, so $R_a \geq R_c$. It is the magnitude of underestimation of R_a by the identified risk R_c that is to be assessed.

K.2 A RESTATEMENT TO MAKE THE PROBLEM TRACTABLE

The problem as stated is evidently impossible to solve unless more mathematical structure or knowledge is assumed. Reasonable added assumptions are sought to make the problem solvable yet realistic.

Suppose that for each $\omega \in \Omega$ there is a probability $d(\omega)$ of detecting the specific ω by safety analysis tools in a reasonable time period. Suppose that $d(\omega)$ depends only upon the particular sequence ω and is independent of all others. Then the safety analysis tools will give exactly one observation of the random quantity

$$Z = \sum_{\omega \in \Omega} r(\omega) X(\omega). \quad (2)$$

For each $\omega \in \Omega$, $X(\omega)$ is a binary variable defined by

$$X(\omega) = \begin{cases} 1 & \text{with probability } d(\omega) \\ 0 & \text{with probability } 1 - d(\omega). \end{cases} \quad (3)$$

This variable indicates whether or not ω has been identified. The quantity $d(\omega)$ is the probability of detecting the sequence ω by the procedure utilized.

We now proceed with the mathematical development of the problem of estimating the actual risk under various assumptions about $d(\omega)$.

K.3 ESTIMATION OF UNIDENTIFIED RISK BASED ON VARIOUS ASSUMPTIONS

Case 1: The Probability of Oversight Is a Constant

Let us examine the results of assuming a constant probability of overlooking each release sequence. Although this model is almost trivial, it is an instructive starting point for developing more meaningful models.

Assuming that $d(\omega) \equiv d$ for $\omega \in \Omega$, it follows from Equations (2) and (3) that, in expectation,

$$EZ = d \sum_{\omega \in \Omega} r(\omega) = d R_a.$$

Thus, based on the theoretical interpretation above, the quantity

$$R = R_c/d \tag{4}$$

is an unbiased estimate of the actual risk R_a .

Note that in order to obtain this estimate, the value of d must be supplied from physical or engineering knowledge. It cannot be determined by statistical estimation. However, a lower bound will suffice for $d(\omega)$ for $\omega \in \Omega$.

If we can assert that

$$P[X(\omega) = 1] \geq d$$

for all $\omega \in \Omega$,

then Equation (4) becomes an estimate such that

$$EZ \geq d R_a.$$

Thus R provides, in expectation, an upper bound for the actual risk R_a .

Case 2: The Probability of Oversight Is a Function of the Risk of the Sequence

Assume that the detection probability is a function of the risk of the release sequence or can be bounded below by some function of the risk. In particular, assume there exist known constants $\kappa > 0$, $\epsilon > 0$ such that

$$d(\omega) \geq \kappa [r(\omega)]^\epsilon$$

for $\omega \in \Omega$.

Then

$$EZ = \sum_{\omega \in \Omega} r(\omega) d(\omega) \geq \kappa \sum_{i=1}^N (r_i)^{1+\epsilon}$$

where, for notational convenience, we write $r_i = r(\omega_i)$ for $i = 1, \dots, N$. This bound can be reduced even further, since $r_i^{1+\epsilon} > r_i$. In this case it becomes identical with the model in Case 1 with $\kappa = d$. For any non-negative random variable Y

$$E(Y^{1+\epsilon}) \geq (EY)^{1+\epsilon}.$$

If we set $Y = r_i$ with probability $1/N$ for $i = 1, \dots, N$, then these inequalities can be combined and expressed as

$$EZ \geq \frac{\kappa}{N^\epsilon} \left(\sum_{i=1}^N r_i \right)^{1+\epsilon} = \frac{\kappa}{N^\epsilon} R_a^{1+\epsilon}.$$

Thus, based on the expected identified risk, a bound on the actual risk is

$$R_a \leq \left[\frac{N^\epsilon}{\kappa} (EZ) \right]^{\frac{1}{1+\epsilon}}.$$

Thus the estimator

$$R = \left(\frac{N^\epsilon}{\kappa} R_c \right)^{\frac{1}{1+\epsilon}} \quad (b)$$

provides an appropriate upper bound on the actual risk R_a .

In this instance the additional information which must be provided by engineering or physical knowledge is either a value for the ratio N/n or an upper bound $A \geq N/n$.

If A is provided, the estimate

$$R = \left[\frac{(nA)^\epsilon}{\kappa} R_C \right] \frac{1}{1 + \epsilon},$$

based on the identified risk, provides an upper bound on R_a in the same sense as before.

Case 3: The Probability of Oversight Is a Function of the Probability of Occurrence of the Sequence

Assume that the detection probability is a function of the probability of the occurrence of the release sequence. We again presume there exist known constants $\kappa > 0$, $\delta > 0$ such that

$$d(\omega) \geq \kappa [P(\omega)]^\delta.$$

Proceeding as before, we have from Equations (2) and (3), in expectation,

$$EZ \geq \kappa \sum_{i=1}^N p_i^{1+\delta} c_i = \kappa C \sum_{i=1}^N p_i^{1+\delta} (c_i / C)$$

where the total consequence is defined as

$$C = \sum_{i=1}^N c_i = \sum_{\omega \in \Omega} c(\omega).$$

Now,

$$EZ \geq \kappa C \left(\sum_{i=1}^N \frac{p_i c_i}{C} \right)^{1+\delta} = \frac{\kappa R_a^{1+\delta}}{C^\delta}.$$

Thus the estimator

$$R = \left(\frac{C^\delta}{\kappa} R_C \right)^{\frac{1}{1+\delta}} \quad (6)$$

provides an appropriate upper bound on the actual risk R_a .

The additional information that must be provided in this case is the value of the total consequence C.

An alternative bound can be obtained using

$$P_0 = \min_{\omega \in \Omega} P(\omega).$$

P_0 is the minimum probability over all sequences in Ω , whether they are found or not. There follows

$$EZ \geq \kappa \sum_{i=1}^N P_i^{1+\delta} c_i \geq \kappa P_0^\delta R_a.$$

The additional information needed in this instance is a lower bound on the probability for all failure sequences in Ω . Thus the estimate

$$R = \frac{R_c}{\kappa P_0^\delta} \quad (7)$$

provides, in expectation, an upper bound on the actual risk.

K.4 APPLICATION OF THE THREE TECHNIQUES

These alternative bounds were compared for one major branch of the WFP preliminary fault tree for liquid waste transfer. The following data are from the 30 cut sets identified. (The data are presented only for illustrative purposes. Their values have little significance because CCF analysis of the fault tree has not yet been performed.)

Total identified risk* (R_c)	8.13×10^{-12} g/yr.
Total identified consequence	49.4 g.
Largest risk of any identified cut set	6.75×10^{-12} g/yr.
Largest probability of any identified cut set	1.41×10^{-12} /yr.
Smallest risk of any identified cut set	1.35×10^{-23} g/yr.
Smallest probability of any identified cut set	9.0×10^{-21} /yr.

* The risk values used here are actually values of the risk measure $A \times B$, in terms of grams released per year.

Case 1:

If the probability of detection of each failure sequence is assumed to be $d = 0.9$, then the estimated actual risk is

$$R = R_c / 0.9 = 9.03 \times 10^{-12} \text{ g/yr.}$$

If the probability of detection is such that $d(\omega) \geq \frac{1}{2}$, then the estimated actual risk is less than

$$R = 2 R_c = 1.626 \times 10^{-11} \text{ g/yr.}$$

The limitation of this case is that the estimated total risk is directly proportional to the inverse of d . This type of relationship results in highly uncertain estimates of R .

Case 2:

Suppose constants κ and ϵ are chosen such that

$$\kappa \times 10^{-22} \epsilon = \frac{1}{2}, \quad \kappa \times 10^{-11} \epsilon = 1.$$

The supposition here is that the probability of detecting the highest risk sequence discovered was close to one, while that of detecting the lowest risk sequences discovered was about $1/2$. Solving the equations above yields

$$\kappa = 2.0000 \quad \epsilon = 2.7366 \times 10^{-2}$$

Thus the calculated probability of detection for the highest risk sequence is 0.99 while that for the lowest risk sequence is 0.47. Calculation by means of Equation (5) yields, for various values of N (total number of failure sequences),

$N = 50,$	$R = 9.07 \times 10^{-12} \text{ g/yr.}$
$N = 100,$	$R = 9.24 \times 10^{-12} \text{ g/yr.}$
$N = 1000,$	$R = 9.83 \times 10^{-12} \text{ g/yr.}$

It is evident that the estimated total risk here is far from being linear with N , a very important result.

Case 3:

The constants κ , δ are again chosen so that the probabilities of detection of the highest probability sequence and of the lowest are near 1 and $\frac{1}{2}$, respectively. Suppose constants κ and δ are chosen such that

$$\kappa(1.5 \times 10^{-11})^\delta = 1, \quad \kappa \times 10^{-19} \delta = 0.5.$$

The solution is

$$\kappa = 2.5033, \quad \delta = 3.6818 \times 10^{-2},$$

and the corresponding highest and lowest detection probabilities are 0.92 and 0.46, respectively. Calculation by means of Equation (7) yields, for various values for P_0 (minimum probability of occurrence of any sequence)

$$P_0 = 10^{-23}, \quad R = 2.28 \times 10^{-11} \text{ g/yr.}$$

$$P_0 = 10^{-25}, \quad R = 2.70 \times 10^{-11} \text{ g/yr.}$$

Using the same values for κ , δ , but assuming various bounds on the total consequence C , yields via Equation (6)

$$C = 100, \quad R = 9.78 \times 10^{-12} \text{ g/yr.}$$

$$C = 200, \quad R = 1.00 \times 10^{-11} \text{ g/yr.}$$

If the assumptions for any of these three cases are at all realistic, then R_a is no more than 5 to 10 times as large as R_c . Thus the accuracy of the estimate of total risk is probably limited more by uncertainties in evaluating identified sequences than by omission of sequences. This is an important conclusion which helps to justify the present effort to bound the risk sum of the unidentified sequences.

APPENDIX L

A FAULT TREE ILLUSTRATING THE TO/THROUGH CONSTRUCTION TECHNIQUE

APPENDIX L

A FAULT TREE ILLUSTRATING THE TO/THROUGH CONSTRUCTION TECHNIQUE

This appendix presents an illustration of the to/through technique for constructing fault trees for nuclear fuel cycle operations. Figure L.1 shows the WFP preliminary fault tree for solidification of high-level liquid waste. The solidification process is based on spray calcination, followed by fusion of the calcine and frit into a glass-ceramic form in stainless steel canisters. The canisters are sealed by welding.

The caption for each page of the fault tree describes the uppermost event appearing on the page. For ease in following the tree from one page to another, "transfer in" symbols are accompanied by an indication of the page on which corresponding "transfer out" symbols are found. The top levels of the fault tree are shown on Page 1 of the tree.

FIGURE L.1, Page 3. Solidification Tree Component for the Existence of Radioactive Material from the Solidification Process (RMS) in the Building Air

FIGURE L.1, Page 4. Solidification Tree Component for the Passage of Air Through the Building Structure

FIGURE L.1, Page 5. Solidification Tree Component for Release of RMS from the Cooling Tower

FIGURE L.1, Page 6. Solidification Tree Component for the Penetration of the Building HEPA

FIGURE L.1, Page 7. Solidification Tree Component for the Penetration of the Off-Gas Cell HEPA

FIGURE L.1, Page 8. Solidification Tree Component for the Penetration of the Solidification Cell HEPA

FIGURE L.1, Page 9. Solidification Tree Component for the Penetration of the Off-Gas HEPA

FIGURE L.1, Page 10. Solidification Tree Component for the Passage of Radioactive Material (RM) Through the Off-Gas Cell

FIGURE L.1, Page 11. Solidification Tree Component for the Passage of Air Through the Solidification Hot Cell Structure

FIGURE L.1, Page 12. Solidification Tree Component for the Release of Radioactive Material into the Solidification Hot Cell Air Due to Calciner Breach

FIGURE L.1, Page 13. Solidification Tree Component for the Release of Radioactive Material into the Solidification Hot Cell Air Due to Leakage Through Calclner Joints and Penetration Following Pressurization

FIGURE L.1, Page 14. Solidification Tree Component for the Release of Radioactive Material into the Solidification Hot Cell Air Due to Release from Canister

FIGURE L.1, Page 15. Solidification Tree Component for the Release of Radioactive Material into the Solidification Hot Cell Air Due to Surge Tank Breach

FIGURE L.1, Page 16. Solidification Tree Component for the Release of Radioactive Material into the Solidification Hot Cell Air Due to Liquid Waste Transfer Piping Leakage

FIGURE L.1, Page 17. Solidification Tree Component for the Release of Radioactive Material into the Solidification Hot Cell Air Due to Melter Failures

DISTRIBUTION

No. of
Copies

No. of
Copies

OFFSITE

UNITED STATES

A. A. Churm
ERDA Chicago Patent Group
9800 South Cass Avenue
Argonne, IL 60439

S. H. Smiley
Deputy Director for Fuels and
Materials
NRC Directorate of Licensing
for Fuels and Materials
4915 St. Elmo Ave.
Bethesda, MD 20014

R. B. Chitwood
Chief, Technical Support Branch
for Fuels and Materials
NRC Directorate of Licensing
for Fuels and Materials
4915 St. Elmo Ave.
Bethesda, MD 20014

W. P. Bishop
Chief, Waste Management Branch
NRC Division of Materials and
Fuel Cycle Facility Licensing
Washington, DC 20555

F. Swanberg
NRC Office of Standards
Development
Washington, DC 20545

C. B. Bartlett
NRC Office of Nuclear Regulatory
Research
Washington, DC 20545

M. Cullingford
NRC Office of Nuclear Regulatory
Research
Washington, DC 20545

S. Levine
NRC Office of Nuclear Regulatory
Research
Washington, DC 20545

W. E. Vesely
NRC Office of Nuclear Regulatory
Research
Washington, DC 20545

I. B. Wall
NRC Office of Nuclear Regulatory
Research
Washington, DC 20545

H. Glauberman
ERDA Division of Environmental
Control Technology
Washington, DC 20545

H. Hollister
ERDA Division of Environmental
Control Technology
Washington, DC 20545

M. S. Kearney
ERDA Division of Environmental
Control Technology
Washington, DC 20545

W. E. Mott
ERDA Division of Environmental
Control Technology
Washington, DC 20545

F. P. Baranowski
ERDA Division of Nuclear Fuel
Cycle and Production
Washington, DC 20545

2 G. H. Daly
ERDA Division of Nuclear Fuel
Cycle and Production
Washington, DC 20545

No. of
Copies

2 O. P. Gormley
ERDA Division of Nuclear Fuel
Cycle and Production
Washington, DC 20545

C. W. Kuhlman
ERDA Division of Nuclear Fuel
Cycle and Production
Washington, DC 20545

A. F. Perge
ERDA Division of Nuclear Fuel
Cycle and Production
Washington, DC 20545

3 R. W. Ramsey
ERDA Division of Nuclear Fuel
Cycle and Production
Washington, DC 20545

E. E. Sinclair
Assistant Director for
Reactor Technology
ERDA Division of Reactor
Research and Development
Washington, DC 20545

W. H. McVey
Chief, Fuel Recycle Branch
ERDA Division of Reactor
Research and Development
Washington, DC 20545

K. K. Kennedy
ERDA Idaho Operations Office
P.O. Box 2108
Idaho Falls, ID 83401

W. F. Hendrickson
ERDA Idaho Operations Office
P.O. Box 2108
Idaho Falls, ID 83401

No. of
Copies

E. H. Hardison
ERDA Oak Ridge Operations Office
P.O. Box X
Oak Ridge, TN 37830

O. T. Turmelle
ERDA Oak Ridge Operations Office
P.O. Box X
Oak Ridge, TN 37830

R. L. Chandler
ERDA Savannah River Operations
Office
P.O. Box A
Aiken, SC 29801

27 ERDA Technical Information Center

J. A. Buckham
Allied Chemical Corporation
550 - 2nd Street
Idaho Falls, ID 83401

A. Schneider
Allied-Gulf Nuclear Services
P.O. Box 847
Barnwell, SC 29812

M. J. Steindler
Argonne National Laboratory
9700 South Cass Ave.
Argonne, IL 60439

F. J. Balkovetz
Aerojet Nuclear Company
550 Second Street
Idaho Falls, ID 83401

G. R. Burdick
Aerojet Nuclear Company
550 Second Street
Idaho Falls, ID 83401

No. of
Copies

E. S. Bartlett
Battelle Memorial Institute
505 King Ave.
Columbus, OH 43201

J. J. Reilly
Brookhaven National Laboratory
Research Library,
Reference Section
Information Division
Upton, Long Island, NY 11973

R. H. Wiswall
Brookhaven National Laboratory
Research Library,
Reference Section
Information Division
Upton, Long Island, NY 11973

Chaim Braun
Brookhaven National Laboratory
Energy Systems Library
Building 902
Upton, NY 11973

Combustion Division
Combustion Engineering, Inc.
Windsor, CT 06095

M. A. Thompson
Dow Chemical Company (ERDA)
Rocky Flats Division
P.O. Box 888
Golden, CO 80401

C. H. Ice
duPont Company, Aiken (ERDA)
E. I. duPont DeNemours and Co.
Savannah River Laboratory
Aiken, SC 29801

A. A. Johnson
duPont Company, Wilmington (ERDA)
E.I. duPont DeNemours and Co.
Wilmington, DE 19898

No. of
Copies

G. J. Dau
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

F. Gelhaus
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

L. Henning
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

G. S. Lellouche
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

M. Levenson
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

L. Minnick
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

E. Zebroski
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

C. Starr
Electric Power Research Institute
3412 Hillview Ave.
P.O. Box 10412
Palo Alto, CA 94304

No. of
Copies

G. L. Meyer
Environmental Protection Agency
Technology Assessment Div. (AW-559)
Office of Radiation Programs
U.S. Environmental Protection
Agency
Washington, DC 20460

W. D. Rowe
Environmental Protection Agency
Waterside Mall-East (AW-558)
Washington, DC 20460

B. Mann
Environmental Protection Agency
P.O. Box 15027
Las Vegas, NV 89114

R. E. Landreth
Environmental Protection Agency
5555 Ridge Ave.
Cincinnati, OH 45213

G. Jansen
Exxon Nuclear Co., Inc.
Richland, Washington 99352

R. G. Barnes
General Electric Company
175 Curtner Ave.
(M/C 160)
San Jose, CA 95125

K. E. El-Sheikh
General Electric Company
920 DeGuigne (MCS34)
Sunnyvale, CA 94086

E. E. Voiland
General Electric Company
Midwest Fuel Recovery Plant
Route 1, Box 219-B
Morris, IL 60450

No. of
Copies

W. H. Reas
General Electric Company
Vallecitos Nuclear Center
Vallecitos Road
Pleasanton, CA 94566

L. H. Brooks
Gulf Energy and Environmental
Systems
P.O. Box 81608
San Diego, CA 92138

Central Research Library
Document Reference Section
Holifield National Laboratory (ERDA)
Oak Ridge, TN 37830

Central Research Library
Holifield National Laboratory (ERDA)
Oak Ridge, TN 37830

Laboratory Records Dept., HNL
Holifield National Laboratory (ERDA)
Oak Ridge, TN 37830

Laboratory Records Dept., HNL-RC
Holifield National Laboratory
Oak Ridge, TN 37830

D. F. Haas
Institute of System Sciences
3085 North Bay Drive
North Bend, OR 97459

L. J. Johnson
Los Alamos Scientific Laboratory (ERDA)
P.O. Box 1663
Los Alamos, NM 87544

H. E. Lambert
Lawrence Livermore Laboratory
Livermore, CA 94550

No. of
Copies

H. S. Jordan
Los Alamos Scientific
Laboratory (ERDA)
P.O. Box 1663
Los Alamos, NM 87544

S. C. Saunders
Mathematical Analysis
Research Corp.
Box 2616, College Station
Washington State University
Pullman, WA 99163

N. Rasmussen
Massachusetts Institute of
Technology
Cambridge, MA 02139

C. J. Kershner
Monsanto Research Corporation
Mound Laboratory
P.O. Box 32
Miamisburg, OH 45342

P. Lamberger
Monsanto Research Corporation
Mound Laboratory
P.O. Box 32
Miamisburg, OH 45342

D. Cyrus Klingsberg
Technical Secretary
National Academy of Sciences
Committee of Radioactive Waste
Management
National Research Council
2101 Constitution Avenue
Washington, DC 20418

J. P. Duckworth
Plant Manager
Nuclear Fuel Services, Inc.
P.O. Box 124
West Valley, NY 14171

E. D. North, Director of
Technical Administration
Nuclear Fuel Services, Inc.
6000 Executive Blvd., Suite 600
Rockville, MD 20852

No. of
Copies

A. C. Pierce
Environmental Specialist
Nuclear Fuel Services
6000 Executive Blvd., Suite 600
Rockville, MD 20852

W. L. Pearl
Nuclear Water and Waste
Technology, Inc.
P.O. Box 6406
San Jose, CA 95150

J. G. Cline, General Manager
NYS Atomic and Space
Development Authority
230 Park Avenue, Rm. 2425
New York, NY 10017

R. K. Weatherwax, Jr.
Princeton University Aerospace
and Mechanical Sciences Dept.
Princeton, NJ 08540

Frank von Hippel
Princeton University Center
for Environmental Studies,
Engineering School
Princeton, NJ 08540

J. Sivinski
Sandia Laboratories
Albuquerque, NM 87107

W. Weart
Sandia Laboratories
Albuquerque, NM 87107

R. R. Fullwood
Science Applications, Inc.
2680 Hanover St.
Palo Alto, CA 94303

F. L. Leverenz, Jr.
Science Applications, Inc.
2680 Hanover St.
Palo Alto, CA 94303

No. of
Copies

R. C. Erdmann
Science Applications, Inc.
2680 Hanover St.
Palo Alto, CA 94303

B. R. Teer
Transnuclear, Inc.
One North Broadway
White Plains, NY 10601

H. C. Claiborne
Union Carbide Corporation (HNL)
P.O. Box Y
Oak Ridge, TN 37830

D. E. Ferguson
Union Carbide Corporation (HNL)
P.O. Box Y
Oak Ridge, TN 37830

W. C. McClain
Union Carbide Corporation (HNL)
P.O. Box Y
Oak Ridge, TN 37830

P. Rubel
Union Carbide Corporation (HNL)
P.O. Box Y
Oak Ridge, TN 37830

D. Okrent
U.C.L.A.
5532 Boelter Hall
Los Angeles, CA 90024

G. E. Apostolakis
U.C.L.A.
5532 Boelter Hall
Los Angeles, CA 90024

S. E. Logan
University of New Mexico
Albuquerque, NM 87131

No. of
Copies

J. B. Fussell
University of Tennessee
Department of Nuclear
Engineering
Knoxville, TN 37916

B. R. Judd
Stanford Research Institute
Menlo Park, CA 94025

R. Howard
Stanford University
Stanford, CA 93045

W. J. VanSlyke
2549 Harris Ave.
Richland, WA 99352

No. of
Copies

FOREIGN

Rene Amavis
EURATOM
Health Physics Division
29, Rue Aldringer
Luxembourg, BELGIUM

K. D. B. Johnson
Atomic Energy Research
Establishment
Harwell, Didcot,
Berks, ENGLAND

D. W. Clelland
United Kingdom Atomic Energy
Authority
Risley, ENGLAND

E. R. Merz
Institut für Chemische
Technologie
Kernforschungsanlage
Jülich GmbH
D517 Jülich
Postfach 365
GERMANY

K. H. Rattay
Institut für Chemische
Technologie
Kernforschungsanlage
Jülich GmbH
D517 Jülich
Postfach 365
GERMANY

W. Heimerl
Institut für Chemische
Technologie
Kernforschungsanlage
Jülich GmbH
Postfach 1913
GERMANY

No. of
Copies

W. A. Issel
KEWA Kernbrennstoff-Wiederaufarbeitungs-
Gesellschaft m.b.H.
Projektleitung
7501 Leopoldshafen
Postfach 60
GERMANY

H. Krause
Nuclear Research Center
Waste Management Department
D75 Karlsruhe
Weberstr. 5
GERMANY

H. Witte
NUKEM GmbH
645 Hanau 11
Postfach 110080
WEST GERMANY

H. J. Wingender
NUKEM GmbH
645 Hanau 11
Postfach 110080
WEST GERMANY

H. Dyroff
NUKEM GmbH
645 Hanau 11
Postfach 110080
WEST GERMANY

Willy Bocola
Laboratorio di Ingegneria Sanitaria
Via Anguillarese km 1 + 300
Roma, ITALY

Ferruccio Gera
Laboratorio Rifiuti Radioattivi
C.N.E.N. - C.S.N. Casaccia
Casella Postale 2400
00100 Rome, ITALY

No. of
Copies

H. W. M. Braun
C.C.R. EURATOM
21020 Ispra (Va)
C.P. 5
ITALIA

Bhabha Atomic Research Centre
Waste Treatment Division
Trombay, Bombay, INDIA

2 International Atomic Energy
Agency
Kärtner Ring 11
P. O. Box 590
A-1011, Vienna, AUSTRIA

H. F. Ramdohr
c/o Friedrich Uhde GmbH
46 Durtmund
Deggingstr. 10-12
GERMANY

M. Stammeler
Battelle-Institute e.v.
6000 Frankfurt am Main 90
Am Romerhuf 35
Frankfurt GERMANY

ONSITE

6 ERDA Richland Operations Office

O. J. Elgert
R. B. Goranson
N. T. Karagianes
R. D. Fogerson
D. J. Squires
F. R. Standerfer

5 Atlantic Richfield Hanford Co.

D. R. Gustafson
R. E. Isaacson
J. H. Warren
D. D. Wodrich
File Copy

1 Exxon

S. J. Beard

No. of
Copies

1 Joint Center for Graduate Study

J. Cooper

2 United Nuclear Industries, Inc.

P. A. Crosetti
A. P. Larrick

5 HEDL

A. G. Blasewitz
C. R. Cooley
J. E. Ecker
J. W. Hagen
W. W. Little

75 Battelle-Northwest

T. W. Ambrose
J. W. Bartlett
R. J. Bashor
H. C. Burkholder
S. H. Bush
N. E. Carter
J. R. Carrell
E. A. Eschbach
J. W. Finnigan
J. C. Fox
J. J. Fuquay
R. J. Hall
L. V. Kimmel
M. R. Kreiter
R. C. Liikala
J. L. McElroy
T. I. McSweeney
E. S. Murphy
R. E. Nightingale
D. E. Olesen
P. J. Pelto
A. M. Platt
J. A. Powell
W. L. Purcell

No. of
Copies

Battelle-Northwest (cont.)

K. J. Schneider
G. D. Seybold
T. H. Smith (15)
D. L. Stevens
J. M. Taylor
L. D. Williams
W. K. Winegardner (25)
Technical Information (5)
Technical Publications